Symantec™ Gateway Security 300 Series Administrator's Guide

Supported models:

Models 320, 360, and 360R

Symantec™ Gateway Security 300 Series Administrator's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.0
February 11, 2004

Copyright notice

Copyright © 1998–2004 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide

Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

See "Licensing" on page 145 for information on the licenses for this product.

Contacting Technical Support

Customers with a current maintenance agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp/.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.
When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec

- Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com/techsupp/, select the appropriate Global Site for your country, then select the enterprise Continue link. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1 Introducing the Symantec Gateway Security 300 Series

Intended audience 12
Where to get more information 12

Chapter 2 Administering the security gateway

Accessing the Security Gateway Management Interface 13
Using the SGMI 15
Managing administrative access 15
Setting the administration password 16
Configuring remote management 17
Managing the security gateway using the serial console 19

Chapter 3 Configuring a connection to the outside network

Network examples 24
Understanding the Setup Wizard 27
About dual-WAN port appliances 27
Understanding connection types 28
Configuring connectivity 30
DHCP 30
PPPoE 31
Static IP and DNS 34
PPTP 36
Dial-up accounts 39
Configuring advanced connection settings 43
Advanced DHCP settings 43
Advanced PPP settings 44
Maximum Transmission Unit (MTU) 45
Configuring dynamic DNS 45
Forcing dynamic DNS updates 47
Disabling dynamic DNS 48
Configuring routing 48
Enabling dynamic routing 48
Configuring static route entries 49
Configuring advanced WAN/ISP settings 50
High availability 50

Load balancing 51
SMTP binding 52
Binding to other protocols 52
Failover 52
DNS gateway 53
Optional network settings 54

Chapter 4 Configuring internal connections

Configuring LAN IP settings 57
Configuring the appliance as DHCP server 58
Monitoring DHCP usage 60
Configuring port assignments 60
Standard port assignment 61

Chapter 5 Network traffic control

Planning network access 63
Understanding computers and computer groups 64
Defining computer group membership 65
Defining computer groups 67
Defining inbound access 68
Defining outbound access 69
Configuring services 72
Redirecting services 73
Configuring special applications 74
Configuring advanced options 76
Enabling the IDENT port 76
Disabling NAT mode 77
Enabling IPsec pass-thru 77
Configuring an exposed host 78
Managing ICMP requests 79

Chapter 6 Establishing secure VPN connections

About using this chapter 82
Creating security policies 82
Understanding VPN policies 82
Creating custom Phase 2 VPN policies 84
Viewing VPN Policies List 85
Identifying users 85
Understanding user types 86
Defining users 86
Viewing the User List 88
Configuring Gateway-to-Gateway tunnels 88

Understanding Gateway-to-Gateway tunnels 88
Configuring dynamic Gateway-to-Gateway tunnels 91
Configuring static Gateway-to-Gateway tunnels 93
Sharing information with the remote gateway administrator 96
Configuring Client-to-Gateway VPN tunnels 96
Understanding Client-to-Gateway VPN tunnels 97
Defining client VPN tunnels 99
Setting global policy settings for Client-to-Gateway VPN tunnels 101
Sharing information with your clients 101
Monitoring VPN tunnel status 102

Chapter 7 Advanced network traffic control

How antivirus policy enforcement (AVpe) works 104
Before you begin configuring AVpe 105
Configuring AVpe 106
Enabling AVpe 107
Configuring the antivirus clients 109
Monitoring antivirus status 109
Log messages 110
Verifying AVpe operation 110
About content filtering 111
Special considerations 111
Managing content filtering lists 112
Special considerations 112
Enabling content filtering for LAN 113
Enabling content filtering for WAN 113
Monitoring content filtering 114

Chapter 8 Preventing attacks

How intrusion detection and prevention works 115
Trojan horse protection 116
Setting protection preferences 116
Enabling advanced protection settings 117
IP spoofing protection 117
TCP flag validation 118

Chapter 9 Logging, monitoring and updates

Managing logging 119
Configuring log preferences 120
Managing log messages 124
Updating firmware 124

Automatically updating firmware 125
Upgrading firmware manually 129
Checking firmware update status 133
Backing up and restoring configurations 133
Resetting the appliance 135
Interpreting LEDs 136
LiveUpdate and firmware upgrade LED sequences 139

Appendix A Troubleshooting

About troubleshooting 141
Accessing troubleshooting information 143

Appendix B Licensing

Session licensing for Symantec Gateway Security 300 Series Client-to-Gateway VPN functions 145
Additive session licenses 145
SYMANTEC GATEWAY SECURITY APPLIANCE LICENSE AND WARRANTY AGREEMENT 146

Appendix C Field descriptions

Logging/Monitoring field descriptions 151
Status tab field descriptions 152
View Log tab field descriptions 154
Log Settings tab field descriptions 155
Troubleshooting tab field descriptions 156
Administration field descriptions 157
Basic Management tab field descriptions 158
SNMP tab field descriptions 158
LiveUpdate tab field descriptions 159
LAN field descriptions 160
LAN IP & DHCP tab field descriptions 161
Port Assignment tab field descriptions 162
WAN/ISP field descriptions 162
Main Setup tab field descriptions 164
Static IP & DNS tab field descriptions 165
PPPoE tab field descriptions 166
Dial-up Backup & Analog/ISDN tab field descriptions 167
PPTP tab field descriptions 171
Dynamic DNS tab field descriptions 171
Routing tab field descriptions 174
Advanced tab field descriptions 175

Firewall field descriptions 176
Computers tab field descriptions 177
Computer Groups tab field descriptions 179
Inbound Rules field descriptions 180
Outbound Rules tab field descriptions 181
Services tab field descriptions 182
Special Application tab field descriptions 183
Advanced tab field descriptions 186
VPN field descriptions 187
Dynamic Tunnels tab field descriptions 189
Static Tunnels tab field descriptions 193
Client Tunnels tab field descriptions 197
Client Users tab field descriptions 199
VPN Policies tab field descriptions 200
Status tab field descriptions 202
Advanced tab field descriptions 203
IDS/IPS field descriptions 204
IDS Protection tab field descriptions 205
Advanced tab field descriptions 206
AVpe field descriptions 207
Content filtering field descriptions 210

Index

Chapter 1

Introducing the Symantec Gateway Security 300 Series

This chapter includes the following topics:

- Intended audience
- Where to get more information

The Symantec Gateway Security 300 Series appliances are Symantec's integrated security solution for small business environments, with support for secure wireless LANs.

The Symantec Gateway Security 300 Series provides integrated security by offering six security functions in the base product:

- Firewall
- IPsec virtual private networks (VPNs) with hardware-assisted 3DES and AES encryption
- Antivirus policy enforcement (AVpe)
- Intrusion detection
- Intrusion prevention
- Static content filtering

All features are designed specifically for the small business. These appliances are perfect for stand-alone environments or as a complement to Symantec Gateway Security 5400 Series appliances deployed at hub sites.

All of the Symantec Gateway Security 300 Series models are wireless-capable. They have special wireless firmware and a CardBus slot that can accommodate

an optional functional add-on, consisting of an integrated 802.11 transceiver and antenna, to allow the highest possible integrated security for wireless LANs, when used with clients running the Symantec Client VPN software. LiveUpdate of firmware strengthens the Symantec Gateway Security 300 Series security response, making it a perfect solution for small businesses.

Intended audience

This manual is intended for system managers or administrators responsible for installing and maintaining the security gateway. It assumes that readers have a solid base in networking concepts and an Internet browser.

Where to get more information

The Symantec Gateway Security 300 Series functionality is described in the following manuals:

- *Symantec™ Gateway Security 300 Series Administrator's Guide*
  The guide you are reading, this guide describes how to configure the firewall, VPN, AntiVirus policy enforcement (AVpe), content filtering, IDS, IPS, LiveUpdate, and all other features of the gateway appliance. It is provided in PDF format on the Symantec Gateway Security 300 Series software CD-ROM.
- *Symantec™ Gateway Security 300 Series Installation Guide*
  Describes in detail how to install the security gateway appliance and run the Setup Wizard to get connectivity.
- *Symantec™ Gateway Security 300 Series Quick Start Card*
  This card provides abbreviated instructions for installing your appliance.

Chapter 2

Administering the security gateway

This chapter includes the following topics:

- Accessing the Security Gateway Management Interface
- Managing administrative access
- Managing the security gateway using the serial console

Accessing the Security Gateway Management Interface

Symantec Gateway Security 300 Series management interface is called the Security Gateway Management Interface (SGMI). The SGMI is a standalone management console for locale management and log viewing. This guide describes how to use the SGMI to manage Symantec Gateway Security 300 Series appliances. The SGMI is a browser-based console where you can create configurations, view status, and access logs.

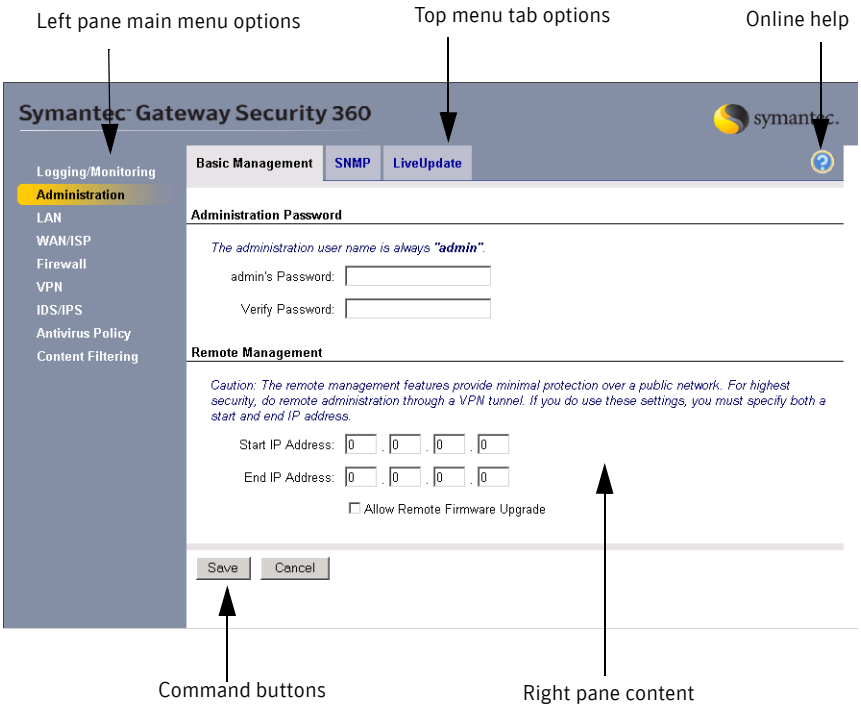
Online help is available for each tab when you click the blue circle with a question mark in the top right corner of each screen.

The SGMI consists of the following features:

- Left pane main menu options
- Right pane menu tabs
- Right pane content
- Right pane command buttons (bottom)
- Help buttons

The Main Menu items are located on the left side of the window at all times.

Figure 2-1 Security Gateway Management Console



Note: The wireless features do not appear in the SGMI until a compatible Symantec Gateway Security WLAN Access Point option is properly installed. See the *Symantec Gateway Security 300 Series Wireless Implementation Guide* for more information.

Use one of the following supported Web browsers to connect to Security Gateway Management Interface:

- Microsoft Internet Explorer version 5.5 or 6.0 SP1
- Netscape version 6.23 or 7.0

You may need to clear the proxy settings in the browser before connecting to the SGMI.

Install the appliance according to the instructions in the *Symantec Gateway Security 300 Series Quick Start Card* before connecting to the SGMI.

The interface you see when you connect to the SGMI may vary slightly depending on the model you are managing. Table 2-1 describes the ports on each model.

Table 2-1 Interfaces by model

Model	Number of WAN ports	Number of LAN ports	Number of serial (modem) ports
320	1	4	1
360/360R	2	8	1

To connect to the SGMI

1. Browse to the IP address of the appliance.
   The default appliance IP address is 192.168.0.1.
2. On your keyboard, press **Enter**.
   The Security Gateway Management Interface window displays.

Using the SGMI

The following list describes how to best work within the SGMI:

- To submit a form, click the appropriate button in the user interface, rather than pressing Enter on your keyboard.
- If you submit a form and receive an error, click the Back button in your Web browser. This retains the data you entered.
- In IP address text boxes, press the Tab key on your keyboard to switch between boxes.
- If after you click a button to submit the form in the user interface the appliance automatically restarts, wait approximately one minute before attempting to access the SGMI again.

Managing administrative access

You manage administrative access by setting a password for the admin user, as well as defining which IP addresses may access the appliance from the wide-area network (WAN) side.

Note: You must set the administration password before you have remote access to the SGMI.

Setting the administration password

The administration password provides secure access to the SGMI. Setting and changing the password limits access to the SGMI to people who have been given the password. You must have installed the appliance and connected your browser to the SGMI to set the password. See the *Symantec Gateway Security 300 Series Installation Guide* for more information about setting up the appliance.

You configure the administration password on the Administration > Basic Management tab or in the Setup Wizard. You can also configure a range of IP addresses from which you can remotely manage the appliance. The administration user name is always admin.

Note: You should change the administration password on a regular basis to maintain a high level of security.

To set the administration password

You set the administration password initially in the Setup Wizard. You can change it in the SGMI, as well as perform a manual reset or reset the appliance through the serial console, which resets the password completely.

Reflashing the appliance with the app.bin version of the firmware resets the password.

See "Upgrading firmware manually" on page 129.

Warning: When you manually reset the password by pressing the reset button, the LAN IP address is reset to the default value (192.168.0.1) and the DHCP server is enabled.

See "Basic Management tab field descriptions" **on page 158.**

To configure a password

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Basic Management tab, under Administration Password, in the Password text box, type the password.
3. In the Verify Password text box, type the password again.
4. Click **Save**.

To manually reset the password

1. On the back of the appliance, press the reset button for 10 seconds.
2. Repeat the configure a password procedure. See "To manually reset the password" on page 17.

Configuring remote management

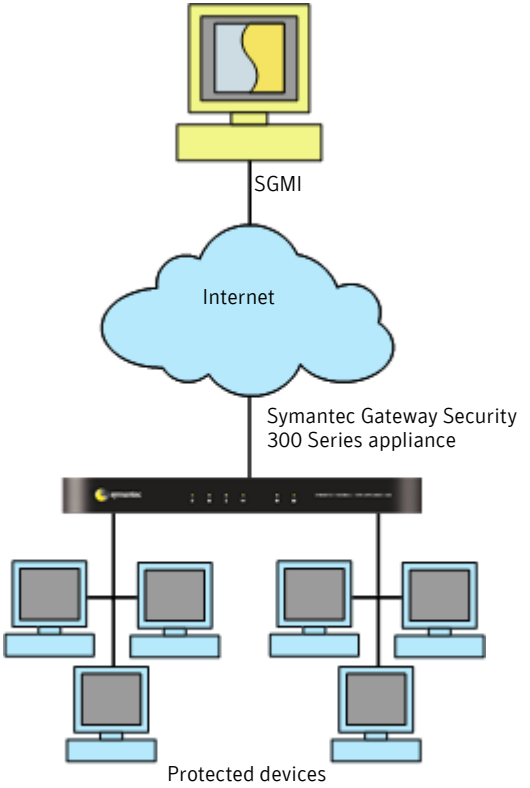
You can access the SGMI remotely from the WAN side using a computer with an IP address that is within configured range of IP addresses. The range is defined by a start and end IP address configured on the Remote Management section on the Administration/Basic Management tab. You should configure the IP address for remote management when you first connect to the SGMI. Remote management is sent in MD5 hash.

Note: For security reasons, you should perform all external remote management through a Gateway-to-Gateway or a Client-to-Gateway VPN tunnel. This provides an appropriate level of confidentiality for your management session.

See "Establishing secure VPN connections" on page 81.

Figure 2-2 shows a remote management configuration.

Figure 2-2 Remote management



To configure remote management, specify both a start and end IP address. If you only want to remotely manage from only one IP address, type it as both the start and end IP address. The start IP address would be the lower number in the range of IP addresses and the end IP address would be the higher number in the range of IP addresses. Leave these fields blank to deny remote access to the SGMI.

To configure for remote management

See "Basic Management tab field descriptions" on page 158.

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the Basic Management tab, under Remote Management, in the Start IP Address text boxes, type the first IP Address (lowest in the range).

3 In the End IP Address text boxes, type the last IP Address (highest in the range).
To permit only one IP address, type the same value in both text boxes.

4 To enable remote Trivial File Transfer Protocol (TFTP) upgrades to the appliance's firmware from the configured IP address range, check **Allow Remote Firmware Upgrade.**
The default is disabled. See "Upgrading firmware manually" on page 129.

5 Click **Save**.

6 To access the SGMI remotely, browse to the <appliance IP address>:8088, where <appliance IP address> is the WAN IP address of the appliance.
When you attempt to access the SGMI remotely, you must log in with the administration user name and password.

Managing the security gateway using the serial console

You can configure or reset the security gateway through the serial port using the null modem cable that is included with the security gateway. Configuring the security gateway in this way is useful for installing in an existing network because it prevents the security gateway from interfering with the network when it is connected.

You can configure a subset of settings through the serial console. These settings include the following:

- LAN IP address (IP address of the security gateway)
- LAN network mask
- Enable or disable the DHCP server
- Range of IP addresses for the DHCP server to allocate

To manage the security gateway using the serial console

1 On the rear of the appliance, connect the null modem cable to the serial port.

2 Connect the null modem cable to your computer's COM port.

3 On the rear of the appliance, turn DIP switch 3 to the on position (up).

4 On your keyboard, ensure that the Scroll Lock is not on.

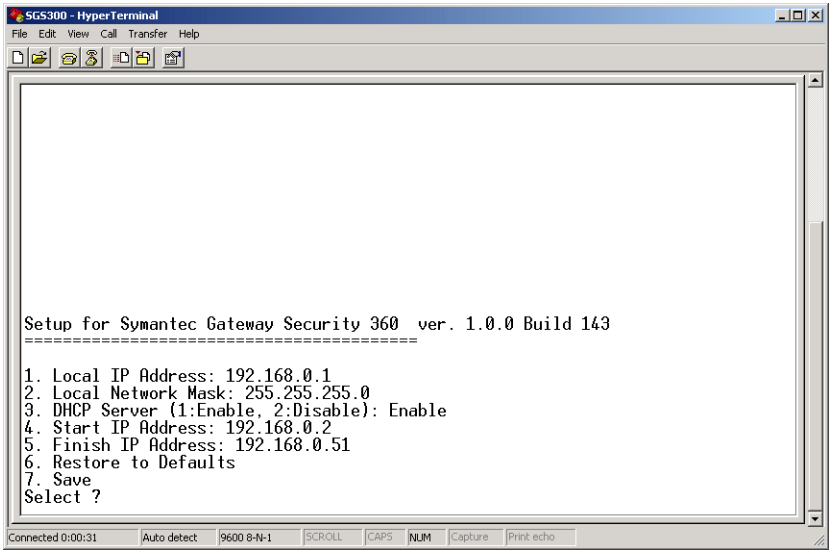
5 Run a terminal program, such as HyperTerminal.

6 In the terminal program, set the program to connect directly to the COM port on your computer to which the appliance is physically connected.

7 Set the communication settings as follows:

Baud (Bits per second)	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

8 Connect to the appliance.



9 After the terminal has connected to the appliance, on the rear panel of the appliance, quickly press the reset button.

10 At the prompt, do one of the following:

Local IP Address	Type 1 to change the IP address of the appliance.
Local Network Mask	Type 2 to change the netmask of the appliance.
DHCP Server	Type 3 to enable or disable the DHCP server feature of the appliance.

Start IP Address	Type 4 to type the first IP address in the range that the DHCP server can allocate.
Finish IP Address	Type 5 to type the last IP address in the range that the DHCP server can allocate.
Restore to Defaults	Type 6 to restore the appliance's default settings for Local IP address, local network mask, DHCP server, and DHCP range.

11 If you are changing local IP address, local network mask, DHCP server, start IP address, or finish IP address, do the following:
   - Type the new value for the setting you are changing.
   - Press **Enter**.
12 If you are restoring the default values for the appliance, press **Enter**.
13 Type **7**.
   The appliance restarts.
14 On the rear of the appliance, turn DIP switch 3 to the off position (down).
15 On the rear of the appliance, quickly press the reset button.

Chapter 3

Configuring a connection to the outside network

This chapter includes the following topics:

- Understanding connection types
- Configuring connectivity
- Configuring advanced connection settings
- Configuring dynamic DNS
- Configuring routing
- Configuring advanced WAN/ISP settings

The Symantec Gateway Security 300 Series WAN/ISP functionality provides connections to the outside world. This can be the Internet, a corporate network, or any other external private or public network. WAN/ISP functionality can also be configured to connect to an internal LAN when the appliance is protecting an internal subnet. Configure the WAN connections as soon as you install the appliance.

You can configure or change the appliance's connectivity on the WAN ports using the WAN/ISP windows or using the Setup Wizard, which is run the first time you access the appliance after you complete the hardware installation.

Before you start configuring a WAN connection, determine what kind of connection you have to the outside network, and based on the connection type, gather information to use during the configuration procedure. See the *Symantec Gateway Security 300 Series Installation Guide* for worksheets to plan the configuration.

Symantec Gateway Security 300 Series model 320 has one WAN port to configure. Models 360 and 360R appliances have two WAN ports that you can

configure separately and differently depending on your needs. Some settings apply to both WAN ports while other settings apply specifically to WAN1 or WAN2.

Warning: After you reconfigure WAN connections and restart the appliance, network traffic is temporarily interrupted. VPN connections are reestablished.

After you have established basic connectivity, you can configure advanced settings, such as DNS, routing, and high availability/load balancing (HA/LB).

Network examples

Figure 3-1 shows a network diagram of a Symantec Gateway Security 300 Series that is connected to the Internet. The termination point represents any network termination type. This is a device that may be provided by your Internet Service Provider (ISP), or a network switch. The computer used for appliance management is connected directly to the appliance using one of the LAN ports on the appliance, and uses a browser to connect to the Security Gateway

Management Interface (SGMI). The protected network communicates through the Symantec Gateway Security 300 Series appliance to the Internet.

Figure 3-1 Connection to the Internet

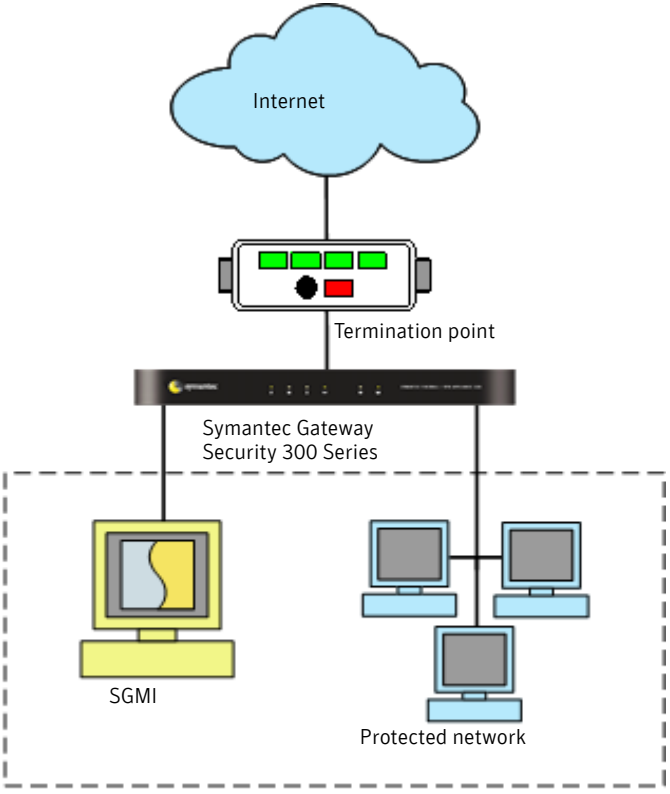
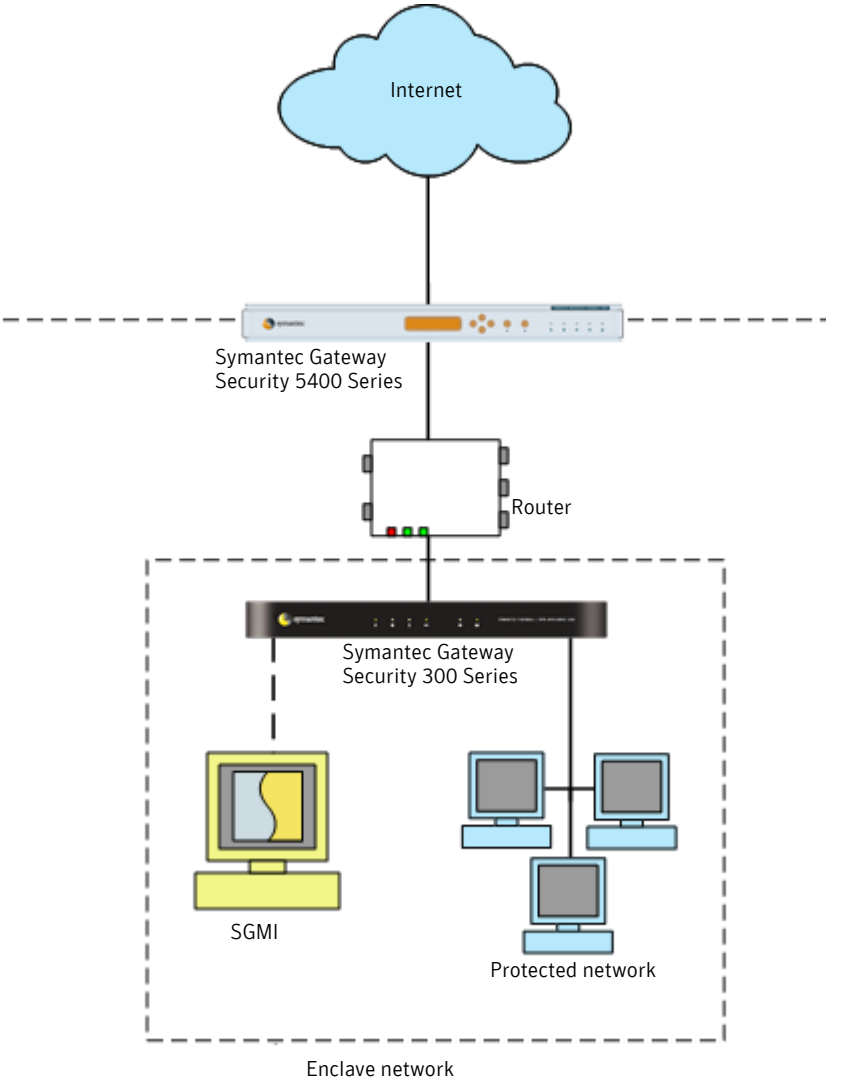


Figure 3-2 shows a network diagram of an appliance connecting to an Intranet. In this scenario, the appliance protects an enclave of the larger internal network from unauthorized internal users. Enclave traffic from the protected network passes through the Symantec Gateway Security 300 Series and through the Symantec Gateway Security 5400 Series to the Internet.

Figure 3-2 Connection to internal network



Understanding the Setup Wizard

The Setup Wizard launches when you first browse to the appliance. The Setup Wizard helps you configure basic connectivity to the Internet or your intranet. If you have already successfully run the Setup Wizard and verified WAN connectivity to the outside network, you do not need to do any additional setup for WAN 1. For models 360 or 360R, use the SGMI to configure WAN 2. See the *Symantec Gateway Security 300 Series Installation Guide* for more information about using the Setup Wizard.

Note: To change the language in which the SGMI appears, rerun the Setup Wizard and select a different language.

The Setup Wizard verifies the current status of the WAN 1 connection before proceeding. If the WAN port (called WAN 1 on models 360 and 360R) is connected to an active network, the Setup Wizard guides you through configuring LiveUpdate and the administration password. If the WAN port is not currently active, the Setup Wizard guides you through entering your ISP-specific connection parameters. Use the WAN/ISP tabs to configure advanced connection settings or to configure WAN 2 port.

You can re-run the Setup Wizard at any time after the initial installation. To run the Setup Wizard, on the WAN/ISP > Main Setup window, click Run Setup Wizard. See the *Symantec Gateway Security 300 Series Installation Guide* for more information.

Warning: Anything you type and save on the WAN/ISP tabs overwrites what you entered previously in the Setup Wizard. This may cause loss of WAN connectivity.

About dual-WAN port appliances

Symantec Gateway Security 300 Series models 360 and 360R appliances have two WAN ports, WAN 1 and WAN 2. The model 360 and 360R appliances support different types of network settings on each of its WAN ports. For example, you may have a static IP account through your business as the primary WAN connection and a secondary (and less expensive) dynamic IP account for a backup connection. Each WAN port is treated as a completely different connection.

Some configurations apply to both WAN ports and for other configurations you must configure each WAN port separately. Table 3-1 indicates the configuration

and whether it applies to both WAN ports or if you must configure each separately.

Table 3-1 WAN port configurations

Configuration	Which WAN port?
Connection types	Configure a connection type for each WAN port. See "Understanding connection types" on page 28.
Backup account	You can configure a primary connection for WAN1 and then connect a modem to the serial port on the back of the appliance for a backup connection. See "Dial-up accounts" on page 39.
Optional network settings	You can specify different configurations for each WAN port. See "Optional network settings" on page 54.
Dynamic DNS	Applies to both WAN1 and WAN2. See "Configuring dynamic DNS" on page 45.
DNS Gateway	Applies to both WAN1 and WAN2. See "DNS gateway" on page 53.
Alive Indicator	Configure an alive indicator for each WAN port. "Dial-up accounts" on page 39 or "Configuring advanced WAN/ISP settings" on page 50.
Routing	Configure routing for each WAN port. See "Configuring routing" on page 48.
WAN port load balancing and bandwidth aggregation	Set the percentage of traffic you want sent through WAN1; the remainder goes through WAN2. See "Load balancing" on page 51.
Bind SMTP	Bind SMTP to either WAN1 or WAN2. See "SMTP binding" on page 52.
High availability	Specify whether high availability is used for each port. See "High availability" on page 50.

Understanding connection types

To connect the appliance to an outside or internal network, you must understand your connection type.

First, determine if you have a dial-up or broadband account. If you have a dial-up account, proceed to Dialup/ISDN. If you have a dedicated account, determine the connection type by reading the following table, and then proceed to the appropriate configuration section.

Typical dial-up accounts are analog (through a normal phone line connected to an external modem) and ISDN (through a special phone line). Typical broadband accounts are broadband cable, DSL, T1/E1, or T3 connected to a terminal adaptor.

Note: Connect only RJ-45 cables to the WAN ports.

The following tables describe the supported connection types. The Connection type column is the option button you click on the Main Setup tab or in the Setup Wizard. The Services column is the types of accounts or protocols that are associated with the connection type. The Network termination types column lists the physical devices that a particular connection type typically uses to connect to the Internet or a network.

Table 3-2 lists the supported dial-up connection types and ways you can identify them.

Table 3-2 Dial-up connection types

Connection type	Services	Network termination types
Analog or ISDN	Plain Old Telephone Service (POTS)	Analog dial-up modem
	Integrated Services Digital Network (ISDN)	Digital dial-up modem An ISDN modem is sometimes called a terminal adaptor.

If you have a broadband account, refer to Table 3-3 to determine which connection type you have.

Table 3-3 Broadband connection types

Connection type	Services	Network termination types
DHCP	Broadband cable	Cable modem
	Digital Subscriber Line (DSL)	DSL modem with Ethernet cable
	Direct Ethernet connection	Ethernet Cable (usually an enclave network)
PPPoE	PPPoE	ADSL modem with Ethernet cable

Table 3-3 Broadband connection types (Continued)

Connection type	Services	Network termination types
Static IP (Static IP & DNS)	Broadband cable	Cable modem
	Digital Subscriber Line (DSL)	DSL modem
	T1	Channel Service Unit/Digital Service Unit (CSU/DSU)
	Direct Ethernet connection	Ethernet cable (usually an enclave network)
PPTP	PPTP	DSL modem with Ethernet cable

Your ISP or network administrator may also be able to help you determine your connection type.

Configuring connectivity

Once you have determined which kind of connection you have, you can configure the appliance to connect to the Internet or intranet using the settings appropriate for that connection.

DHCP

Dynamic Host Configuration Protocol (DHCP) automates the network configuration of computers. It enables a network with many clients to extract configuration information from a single server (DHCP server). In the case of a dedicated Internet account, the users are the clients extracting information from the ISP's DHCP server, and IP addresses are only assigned to connected accounts.

The account you have with your ISP may use DHCP to allocate IP addresses to you. Account types that frequently use DHCP are broadband cable and DSL. ISPs may authenticate broadband cable connections using the MAC address or physical address of your computer or gateway.

See "Configuring connectivity" on page 30 for information on configuring DHCP to allocate IP addresses to your nodes.

Before configuring DHCP for your WAN ports, you must select DHCP (Auto IP) as your connection type on the Main Setup window.

To select DHCP as your connection type

See "Main Setup tab field descriptions" on page 164.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 For model 320, do the following:

- In the right pane, on the Main Setup tab, under Connection Type, click **DHCP**.
- Click **Save**.

3 For model 360 or 360R, do the following:

- To select a connection type for WAN1, under WAN1 (External), in the Connection Type drop-down list, click **DHCP**.
- To select a connection type for WAN2, under WAN2 (External), in the Connection Type drop-down list, click **DHCP**.

4 Click **Save**.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is used by many Asymmetrical Digital Subscriber Line (ASDL) providers. It is a specification for connecting many users on a network to the Internet through a single dedicated medium, such as a DSL account.

You can specify whether you connect or disconnect your PPPoE account manually or automatically. This is useful to verify connectivity.

You can configure the appliance to connect only when an Internet request is made from a user on the LAN (for example, browsing to a Web site) and disconnect when the connection is idle (unused). This feature is useful if your ISP charges on a per-usage time basis.

You can use multiple logins (if your ISP account allows multi-session PPPoE) to obtain additional IP addresses for the WAN. These are called PPPoE sessions. The login may be the same user name and password as the main session or may be different for each session, depending on your ISP. Up to five sessions or IP addresses are allowed for model 320 and up to three sessions for each WAN port on models 360 and 360R. LAN hosts are bound to a session on the Computers tab. See "Configuring LAN IP settings" on page 57.

Note: Multiple IP addresses on a WAN port are only supported for PPPoE connections.

By default, all settings are associated with Session 1. For multi-session PPPoE Accounts, configure each session individually. If you have multiple PPPoE accounts, assign each one to a different session in the SGMI.

Before configuring the WAN ports to use a PPPoE account, gather the following information:

- User name and password
  All PPPoE accounts require user names and passwords. Get this information from your ISP before configuring PPPoE.
- Static IP address
  You may have purchased or are assigned a static IP address for the PPPoE account.

To configure PPPoE

See "PPPoE tab field descriptions" on page 166.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For model 320, do the following:
   - In the right pane, on the Main Setup tab, under Connection Type, click **PPPoE (xDSL)**.
   - Click **Save**.
3. For model 360 or 360R, do the following:
   - In the right pane, on the Main Setup tab, under WAN1 (External), in the Connection Type drop-down list, click **PPPoE (xDSL)**.
   - To use WAN 2, under WAN 2 (External), under HA Mode, click **Normal**.
   - To use WAN2, under WAN2 (External), in the Connection Type drop-down list, click **PPPoE (xDSL)**.
   - Click **Save**.
   - In the right pane, on the PPPoE tab, in the right pane, on the PPPoE tab, under WAN Port and Sessions, do one of the following:
   - On the WAN Port drop-down list, select a WAN port to configure.
4. If you have a multi-session PPPoE account, under WAN Port and Sessions, on the PPPoE Session drop-down list, select the appropriate session.
5. If you have a single-session PPPoE account, leave the PPPoE session at Session 1.
6. Under Connection, check **Connect on Demand**.
   If you want to connect to a PPPoE session manually, uncheck **Connect on Demand**, and then under Manual Control, click **Connect**.

7 In the Idle Time-out text box, type the number of minutes of inactivity after which you want the appliance to disconnect from the PPPoE account.

8 If you have a static IP PPPoE Internet account, in the Static IP Address text box, type the IP address.
Otherwise, leave the value at 0.

9 Under Choose Service, click **Query Services.**
You must be disconnected from your PPPoE account to use this feature.
See "Connecting manually to your PPPoE account" on page 34.

10 From the Service drop-down list, select a PPPoE service.
You must click Query Services to select a service.

11 In the User Name text box, type your PPPoE account user name.

12 In the Password text box, type your PPPoE account password.

13 In the Verify Password text box, retype your PPPoE account password.

14 Click **Save**.

Verifying PPPoE connectivity

Once the appliance is configured to use the PPPoE account, verify that it connects correctly.

To verify connectivity

See "PPPoE tab field descriptions" on page 166.

See "Status tab field descriptions" on page 152.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 In the right pane, on the PPPoE tab, under Manual Control, click **Connect**.

3 In the left pane, click **Logging/Monitoring**.

In the right pane, on the Status tab, under WAN1 (External Port), the connection status is displayed.

If you are not connected, verify the following items:

- You typed your user name and password correctly. Some ISPs expect the user name to be email address format, for example, johndoe@myisp.net.
- Check that all the cables are firmly plugged in.
- Your account information with your ISP and that your account is active.

Connecting manually to your PPPoE account

You can manually connect or disconnect from your PPPoE account. For model 360 or 360R, you can manually control the connection for either WAN port. This is useful to troubleshoot the connection to the ISP.

To manually control your PPPoE account

You can manually control your PPPoE account through the SGMI.

See "PPPoE tab field descriptions" on page 166.

To manually connect to the PPPoE account

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For model 320, in the right pane, on the PPPoE tab, under Manual Control, click **Connect**.
3. For model 360 or 360R, do the following:
   - In the right pane, on the PPPoE tab, under WAN Port and Sessions, in the WAN Port drop-down list, select the WAN port to connect.
   - In the Session drop-down list, select a PPPoE session.
   - Under Manual Control, click **Connect**.

To manually disconnect from the PPPoE account

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For model 320, in the right pane, on the PPPoE tab, under Manual Control, click **Disconnect**.
3. For model 360 or 360R, do the following:
   - In the right pane, on the PPPoE tab, under WAN Port and Sessions, in the WAN Port drop-down list, select the WAN port to disconnect.
   - In the Session drop-down list, select a PPPoE session.
   - Under Manual Control, click **Disconnect**.

Static IP and DNS

When you get an account with an ISP, you may have the option to purchase a static (permanent) IP address. This enables you to run a server, such as a Web or FTP server, because the address remains the same, all the time. Any type account (dial-up or broadband) can have a static IP address.

The appliance forwards any DNS lookup request to the specified DNS server for name resolution. The appliance supports up to three DNS servers. When you

specify multiple DNS servers, they are used in sequence. For example, after the first server is used, the next request is forwarded to the second server and so on.

If you have a static IP address with your ISP or are using the appliance behind another security gateway device, select Static IP and DNS for your connection type. You can specify your static IP address and the IP addresses of the DNS servers you want to use for name resolution.

Before configuring the appliance to connect with your static IP account, gather the following information:

- Static IP, netmask, and default gateway addresses
  Contact your ISP or IT department for this information.
- DNS addresses
  You must specify the IP address for at least one, and up to three, DNS servers. Contact your ISP or IT department for this information. You do not need DNS IP address entries for dynamic Internet accounts or accounts where a DHCP server assigns the IP addresses.
  If you have a static IP address with PPPoE, configure the appliance for PPPoE.

To configure static IP

You must specify the static IP address and the IP address for the DNS that you want to use. You must enter at least one DNS if you have a static IP account.

See "Static IP & DNS tab field descriptions" on page 165.

To configure static IP

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. In the right pane, on the Main Setup tab, under Connection Type, click **Static IP**.
3. Click **Save**.
4. For model 320, do the following:
   - In the right pane, on the Static IP & DNS tab, under WAN IP, in the IP Address text boxes, type the desired IP address of the external (WAN) side of the Symantec Gateway Security 300 Series appliance.
   - In the Network Mask text box, type the network mask.
     Change this only if your ISP requires it.
   - In the Default Gateway text box, type the default security gateway.
   - In the Domain Name Servers text boxes, type the IP address for at least one, and up to three, domain name servers.
   - Click **Save**.

5 For model 360 or 360R, do the following:

- Under WAN1 (External), in the Connection Type drop-down list, click **Static IP**.
- To use WAN 2, under WAN 2 (External), under HA Mode, click **Normal**.
- To use WAN 2, under WAN2 (External), in the Connection Type drop-down list, click **Static IP**.
- Click **Save**.
- In the right pane, on the Static IP & DNS tab, under either WAN 1 IP or WAN2 IP, in the IP Address text boxes, type the desired IP address of the external (WAN) side of the Symantec Gateway Security 300 Series appliances.
- In the Network Mask text box, type the network mask.
- In the Default Gateway text box, type the default security gateway. Symantec Gateway Security 300 Series sends any packet it does not know how to route to the default security gateway.
- In the Domain Name Servers text boxes, type the IP address for at least one, and up to three, domain name servers.

6 Click **Save**.

PPTP

Point-to-Point-Tunneling Protocol (PPTP) is a protocol that enables a secure data transfer from a client to a server by creating a tunnel over a TCP/IP-based network. Symantec Gateway Security 300 Series appliances act as a PPTP access client (PAC) when you connect to a PPTP Network Server (PNS), generally with your ISP.

Before beginning PPTP configuration, gather the following information:

- PPTP server IP address
  IP address of the PPTP server at the ISP.
- Static IP address
  IP address assigned to your account.
- Account information
  User name and password to log in to the account.

To configure PPTP

See "PPTP tab field descriptions" on page 171.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 For model 320, do the following:
   - In the right pane, on the Main Setup tab, under Connection Type, click **PPTP**.
   - Click **Save**.
3 For model 360 or 360R, do the following:
   - Under WAN1 (External), in the Connection Type drop-down list, click **PPTP**.
   - To use WAN 2, under WAN 2 (External), under HA Mode, click **Normal**.
   - To use WAN 2, under WAN2 (External), in the Connection Type drop-down list, click **PPTP**.
   - Click **Save**.
4 In the right pane, on the PPTP tab, under Connection, check **Connect on Demand.**
5 In the Idle Time-out text box, type the number of minutes of inactivity after which you want the appliance to disconnect the PPTP connection.
6 In the Server IP Address text box, type the IP address of the PPTP server.
7 If you have a static IP PPTP Internet account, in the Static IP Address text boxes, type the IP address.
   Otherwise, leave the value at 0.
8 Under User Information, in the User Name text box, type your ISP account user name.
9 In the Password text box, type your ISP account password.
10 In the Verify text box, type your ISP account password.
11 Click **Save**.

Verifying PPTP connectivity

Once the appliance is configured to use the PPTP account, verify that it connects correctly.

To verify PPTP connectivity

See "PPTP tab field descriptions" on page 171.

See "Status tab field descriptions" on page 152.

1 In the SGMI, in the left pane, click **WAN/ISP**.
2 For model 320, in the right pane, on the PPTP tab, under Manual Control, click **Connect**.

3 For model 360 and 360R, do the following:
   - In the right pane, on the PPTP tab, under WAN Port, in the WAN Port drop-down list, select the WAN port to connect.
   - Under Manual Control, click **Connect**.
4 In the left pane, click **Logging/Monitoring**.

In the right pane, on the Status tab, under WAN1 (External Port), the connection status is displayed.

If you are not connected, verify that you have typed your user name and password correctly. If you are still not connected, call your ISP and verify your account information and that your account is active.

Connecting manually to your PPTP account

You can manually connect to or disconnect from your PPTP account. For model 360 or 360R, you can manually control the connection for either WAN port. This is helpful for troubleshooting connectivity.

To manually connect to your PPTP account

For model 320, you can connect or disconnect to your PPTP account. For model 360 or 360R, you select the WAN port to control, and then connect or disconnect.

See "PPTP tab field descriptions" on page 171.

To manually connect your PPTP account

1 In the SGMI, in the left pane, click **WAN/ISP**.
2 For model 320, in the right pane, on the PPTP tab, under Manual Control, click **Connect**.
3 For model 360 or 360R, do the following:
   - In the right pane, on the PPTP tab, under WAN Port, in the WAN Port drop-down list, select the WAN port to connect.
   - Under Manual Control, click **Connect**.

To manually disconnect your PPTP account

1 In the SGMI, in the left pane, click **WAN/ISP**.
2 For model 320, in the right pane, on the PPTP tab, under Manual Control, click **Disconnect**.
3 For model 360 or 360R, do the following:

- In the right pane, on the PPTP tab, under WAN Port, in the WAN Port drop-down list, select the WAN port to connect.
- Under Manual Control, click **Disconnect**.

Dial-up accounts

There are two basic types of dial-up accounts: analog and ISDN. Analog uses a modem that connects to a regular telephone line (RJ-11 connector). ISDN is a digital dial-up account type that uses a special telephone line.

On the appliance, you can use a dial-up account as your primary connection to the Internet, or as a backup to your dedicated account. In backup mode, the appliance automatically dials the ISP if the dedicated connection fails. The appliance re-engages the dedicated account when it is stable; failover from the primary connection to modem or from the modem to the primary connection can take 30 to 60 seconds.

You can configure a primary dial-up account and a backup dial-up account. You may configure a backup dial-up account if your primary dedicated account fails. First, you must connect the modem to the appliance. Then, you use the SGMI to configure the dial-up account.

You can also connect or disconnect your account manually at any time.

You must use an external modem for dial-up accounts. You connect the modem, including ISDN modems, to the appliance through the serial port on the back of the appliance. Figure 3-3 shows the serial port on the rear panel of the model 320 appliance.

Figure 3-3 Rear panel of Symantec Gateway Security model 320 appliance

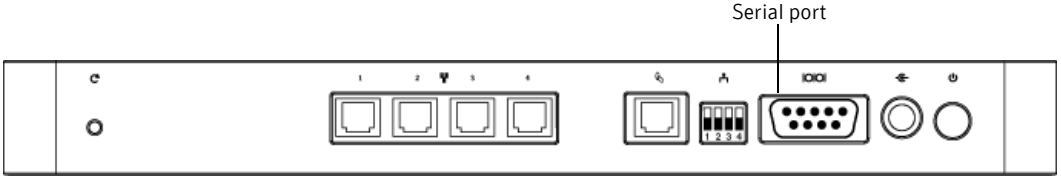
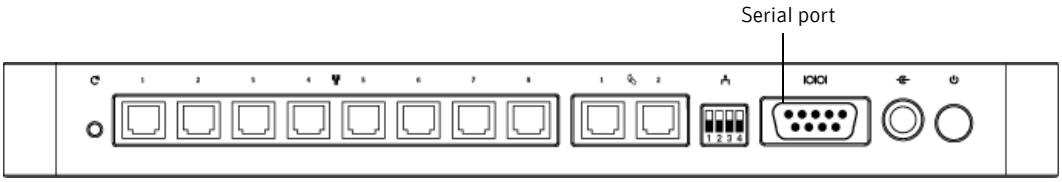


Figure 3-4 shows the serial port on the rear panel of the model 360 and 360R appliances.

Figure 3-4 Rear panel of Symantec Gateway Security model 360 and 360R appliances



Before configuring the appliance to use your dial-up account as either the primary or backup connection, gather the following information and equipment:

Account information	User name, which may be different from your account name, and password for the dial-up account.
Dial-up numbers	At least one, and up to three, telephone numbers for the dial-up account.
Static IP address	Some ISPs assign static IP addresses to their accounts, or you may have purchased a static IP address.
Modem/cables	An external modem and a serial cable to connect the modem to the serial port on the back of the appliance.
Modem documentation	You may need to consult your modem's documentation for modem command or model information.

To configure dial-up accounts

First, you must connect the modem to the appliance. Then, you use the SGMI to configure the dial-up account.

Note: If your ISP gateway blocks ICMP requests such as PING, on the Main Setup tab, if you leave the Alive Indicator Site IP or URL text box blank, the appliance PINGs the default gateway to determine connectivity.

See "Dial-up Backup & Analog/ISDN tab field descriptions" on page 167.

To connect your modem

1. Plug one end of the serial cable into your modem.
2. Plug one end of the serial cable into the serial port on the back of the appliance.
3. If it requires external power, plug the modem into a wall socket.
4. Turn on the modem.

To configure your primary dial-up account

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 In the right pane, on the Main Setup tab, under Connection Type, click **Analog/ISDN**.

3 Click **Save**.

4 On the Dial-up Backup & Analog/ISDN tab, under ISP Account Information, do the following:

User Name	Type the account user name.
Password	Type the account password.
Verify Password	Retype the account password.
Dial-up Telephone 1	Type the dial-up telephone number.
Dial-up Telephone 2	Optionally, type a backup dial-up telephone number.
Dial-up Telephone 3	Optionally, type a backup dial-up telephone number.

5 Under Modem Settings, do the following:

Model	Select the model of your modem.
Line Speed	Select the speed at which you want to connect.
Dial Type	Select the dial type.
Redial String	Type a redial string.
Initialization String	Type an initialization string. If you select a modem type other than Other, the initialization string is provided. If you select Other, you must type an initializatio nstring.
Line Type	Select the type of telephone line.
Dial String	Type a dial string.
Idle Time Out	Type the amount of time, in minutes, after which the connection is closed if idle.

6 Click **Save**.

After you click Save, the appliance restarts. Network connectivity is interrupted.

To enable the backup dial-up account

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Dial-up Backup and Analog/ISDN tab, under Backup Mode, do the following:
   - Check **Enable Backup Mode**.
   - In the Alive Indicator Site IP or URL text box, type the IP address or resolvable name of the site to check connectivity.
3. Under Modem Settings, click **Save**.
4. Follow the steps in "Dial-up accounts" on page 39.

Controlling your dial-up account manually

You can force the appliance to connect or disconnect from your dial-up account. This is helpful for verifying connectivity.

To manually control the dial-up account

See "Dial-up Backup & Analog/ISDN tab field descriptions" on page 167.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. To connect to the dial-up account, on the Dial-up Backup & Analog/ISDN tab, under Manual Control, click **Dial**.
3. To disconnect from the dial-up account, on the Dial-up Backup & Analog/ISDN tab, under Manual Control, click **Hang Up**.

Verifying dial-up connectivity

Once you have configured the appliance to use your dial-up account, verify that it connects correctly.

To verify dial-up connectivity

See "Dial-up Backup & Analog/ISDN tab field descriptions" on page 167.

See "Status tab field descriptions" on page 152.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. In the right pane, on the Dial-up Backup & Analog/ISDN tab, under Manual Control, click **Dial**.
3. In the left pane, click **Logging/Monitoring**.
4. In the right pane, on the Status tab, under WAN1 (External Port), next to Connection Status, your connection status is displayed.

If you are not connected, verify the following information:

- You have typed your user name and password correctly.
- Initialization string is correct for your model modem. Check your modem documentation for more information.
- Cables are securely plugged in.
- Phone jack to which the modem is connected is functioning.
- Verify your account information with your ISP and that your account is active.

Monitoring dial-up account status

You can view and refresh the status of your dial-up account connection.

To monitor dial-up account status

See "Dial-up Backup & Analog/ISDN tab field descriptions" on page 167.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Dial-up Backup & Analog/ISDN tab, scroll to Analog Status.
3. To refresh the dial-up account status, on the Dial-up Backup & Analog/ISDN tab, under Modem Settings, click **Refresh**.

Configuring advanced connection settings

Advanced connection settings let you control your connectivity parameters more closely. If you have a DHCP connection, you can configure the renew settings. For PPPoE accounts, you can configure echo requests. For all connection types, you can specify packet size by setting the Maximum Transfer Unit (MTU).

Advanced DHCP settings

If you selected DHCP as your connection type, you can tell the appliance when to send a renew request, which tells the ISP to allocate a new IP address to the appliance.

You can tell the appliance at any time to request a new IP address, by forcing a DHCP renew. However, you should only do this if requested by Symantec Technical Support.

To configure advanced DHCP settings

You can configure the idle renew time and manually force a DHCP renew request.

See "Advanced tab field descriptions" on page 175.

To configure idle renew

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Advanced tab, under Optional Connection settings, in the Idle Renew DHCP text box, type the number of minutes after which a renew lease request is sent.
3. Click **Save**.

To force a DHCP renew

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For model 320, on the Advanced tab, under Optional Connection settings, click **Force Renew**.
3. For model 360 or 360R, do one of the following:
   - To renew WAN1, on the Advanced tab, under Optional Connection Settings, click **Renew WAN1**.
   - To renew WAN2, on the Advanced tab, under Optional Connection Settings, click **Renew WAN2**.

Advanced PPP settings

You can configure the echo requests that the appliance sends to verify that the appliance is connected to the PPPoE account.

To configure PPP settings

See "Advanced tab field descriptions" on page 175.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Advanced tab, under PPP settings, do the following:
   - In the Time-out text box, type the number of seconds before trying another echo request.
   - In the Retries text box, type the number of times for the appliance to attempt to reconnect.
3. Click **Save**.

Warning: To reset the echo request settings, click Restore Defaults. This also resets the MTU number and the DHCP Idle Renew settings to their default values.

Maximum Transmission Unit (MTU)

You can specify the maximum size of the packets that arrive at and leave the appliance through the WAN port you are configuring. This is useful if a computer or another appliance along the transmission path requires a smaller MTU. On models 360 and 360R, if you are configuring WAN1 and WAN2, you can set a different MTU for each port.

To specify MTU size

See "Advanced tab field descriptions" on page 175.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. In the right pane, on the Advanced tab, under Optional Connection Settings, in the WAN port text box, type the MTU size.
3. Click **Save**.

Warning: To reset the MTU size, click Restore Defaults. This also resets the echo request information and the DHCP Idle Renew settings to their default values.

Configuring dynamic DNS

The Symantec Gateway Security 300 Series can use a dynamic DNS service to map dynamic IP addresses to a domain name to which users can connect.

If you receive your IP address dynamically from your ISP, dynamic DNS services let you use your own domain name (mysite.com, for example) or to use their domain name and your subdomain to connect to your services, such as a a VPN gateway, Web site or FTP. For example, if you set up a virtual Web server and your ISP assigns you a different IP address each time you connect the server, your users can always access www.mysite.com.

The appliances support two types of dynamic DNS services: standard and TZO. You can configure either service by specifying account information, or you can disable dynamic DNS completely.

See the *Symantec Gateway Security 300 Series Release Notes* for the list of supported services.

When you create an account with TZO, they send you the following information to log in and use your account: key (password), email (user name), and domain. Gather this information before configuring the appliance to use TZO. For more information about TZO dynamic DNS, go to http://www.tzo.com.

To use standard service DNS, gather the following information:

- Account information
  User name (which may be different from the account name) and password for the dynamic DNS account.
- Server
  IP address or resolvable name of the dynamic DNS server. For example, members.dyndns.org.

To configure dynamic DNS

For model 320, you can configure the WAN port to use dynamic DNS. For model 360 or 360R, you can configure WAN1, WAN2, or both ports to use dynamic DNS.

See "Dynamic DNS tab field descriptions" on page 171.

See "Main Setup tab field descriptions" on page 164.

To configure TZO dynamic DNS

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Dynamic DNS tab, under Service Type, click **TZO**.
3. Do one of the following:
   - For model 320, skip to step 4.
   - For model 360 and 360R, in the WAN Port drop-down list, select the WAN port for which you are configuring TZO.
4. Under TZO Dynamic DNS Service, do the following:
   - In the Key text box, type the key that TZO sent when the account was created.
   - In the Email text box, type the email address you specified when you created the TZO account.
   - In the Domain text box, type the domain name that TZO handles. For example, marketing.mysite.com.
5. Click **Save**.

To configure standard service DNS

1. In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Dynamic DNS tab, under Service Type, click **Standard**.

3 Do one of the following:

- For model 320, skip to step 4.
- For model 360 and 360R, in the WAN Port drop-down list, select the WAN port for which you are configuring dynamic DNS.

4 Under Standard Service, do the following:

User Name	Type the dynamic DNS account user name.
Password	Type the dynamic DNS account password.
Verify Password	Retype the dynamic DNS account password.
Server	Type the IP address or DNS-resolvable name for the dynamic DNS server.
Host Name	Type the host name that you want to use.

5 Optionally, under Standard Optional Settings, do the following:

- To access your network with *.yourhost.yourdomain.com where * is a CNAME like FTP or www, yourhost is the host name, and yourdomain.com is your domain name, check **Wildcards**.
- To use a backup mail exchanger, check **Backup MX**.
- In the Mail Exchanger text box, type the domain name of the mail exchanger.

6 Click **Save**.

Forcing dynamic DNS updates

When you force a dynamic DNS update, the appliance sends its current IP address, host name, and domain to the service. Do this only if requested by Symantec Technical Support.

For model 320, you can force a dynamic DNS update for the WAN port. For model 360 or 360R, you can force a dynamic DNS update for WAN1, WAN2, or both ports.

To force a DNS update

See "Dynamic DNS tab field descriptions" on page 171.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 For model 320, on the Dynamic DNS tab, under Service Type, click **Update**.

3 For model 360 or 360R, do the following:

- On the Dynamic DNS tab, under Service Type, in the WAN Port drop-down list, select the WAN port for which you are configuring TZO.
- Click **Update**.

Disabling dynamic DNS

You can disable dynamic DNS if you are hosting your own domain. On model 360 or 360R, you can disable dynamic DNS for both WAN ports.

To disable dynamic DNS

See "Dynamic DNS tab field descriptions" on page 171.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. For model 320, on the Dynamic DNS tab, under Service Type, click **Disable**.
3. For model 360 or 360R, do the following:
   - On the Dynamic DNS tab, under Service Type, in the WAN Port drop-down list, select the WAN port to disable.
   - Click **Disable**.
4. Click **Save**.

Configuring routing

If you install Symantec Gateway Security 300 Series appliances on a network with more than one directly connected router, you must specify to which router to send traffic. The appliance supports two types of routing: dynamic and static. Dynamic routing chooses the best route for packets and sends the packets to the appropriate router. Static routing sends packets to the router you specify. Routing information is maintained in a routing table.

Dynamic routing is administered using the RIP v2 protocol. When it is enabled, the appliance listens and sends RIP requests on both the internal (LAN) and external (WAN) interfaces. RIP v2 updates the routing table based on information from untrusted sources, so you should only use dynamic routing for intranet or department gateways where you can rely on trusted routing updates.

Routing helps the flow of traffic when you have multiple routers on a network. Configure dynamic or static routing to fit your needs.

Enabling dynamic routing

You do not need routing information to use dynamic routing.

To enable dynamic routing

See "Routing tab field descriptions" on page 174.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Routing tab, under Dynamic Routing, check **Enable RIP v2**.

3 Click **Save**.

Configuring static route entries

Before adding static routing entries to the routing table, gather the destination IP, netmask, and gateway addresses for the router to which you want traffic to be routed. Contact your IT department for this information.

You can add new route entries, edit existing entries, delete entries, or view a table of entries.

Note: If NAT is enabled, only six routes display in Routing List. When NAT is disabled, all configured routes appear in the list.

To configure static route entries

You can add, edit, or delete a static routing entry, or view the list of existing entries.

See "Routing tab field descriptions" on page 174.

To add a route entry

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Routing tab, under Static Routes, do the following:

Destination IP	Type the IP address to which to send packets.
Netmask	Type the net mask of the router to which to send packets.
Gateway	Type the IP address of the interface to which packets are sent.
Interface	Select the interface from which traffic is sent.
Metric	Type a number to represent the order in which you want the entry evaluated. For example to evaluate the entry third type 3.

3 Click **Add**.

To edit a route entry

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Routing tab, under Static Routes, in the Route Entry drop-down list, select a route entry.
3. Under Static Routes, change information in any of the fields.
4. Click **Update**.

To delete a route entry

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Routing tab, under Static Routes, in the Route Entry drop-down list, select an entry.
3. Click **Delete**.

To view the routing list table

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Routing tab, scroll to the bottom of the page.

Configuring advanced WAN/ISP settings

You can set advanced connectivity settings such as a DNS gateway, HA/LB, SMTP binding, and failover. You can also set optional network settings, which identify the appliance to a network.

Note: Model 320 appliances have one WAN port and do not support high availability, load balancing, and bandwidth aggregation.

High availability

You can configure high availability for each WAN port in one of three ways: Normal, Off, or Backup. Table 3-4 describes each mode.

Table 3-4 High availability modes

Mode	Description
Normal	Load balancing settings apply to the port when it is enabled and operational.
Off	WAN port is not used at all.

Table 3-4 High availability modes

Mode	Description
Backup	WAN port only passes traffic if the other WAN port is not functioning.

By default, WAN1 is set to Normal and WAN2 is set to Off.

Bandwidth aggregation lets you combine the amount of traffic that goes over WAN1 and WAN2 to increase the amount of bandwidth your clients can use. For WAN data transfer, data aggregation can provide up to double the WAN throughput, depending on traffic characteristics.

To configure high availability

See "Main Setup tab field descriptions" on page 164.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Main Setup tab, do the following:

- To configure the WAN1 port, under WAN1, select a high availability mode.
- To configure the WAN2 port, under WAN2, select a high availability mode.

3 Click **Save.**

Load balancing

Symantec Gateway Security 300 Series model 360 and 360R appliances each have two WAN ports. On these appliances, you can configure high availability and load balancing (HA/LB) between the two WAN ports.

You can set the percentage of packets that is sent over WAN1 or WAN2. You enter a percentage only for WAN1; the remainder of the packets are then sent over WAN2. If you have a slower connection, use a lower value for that WAN port for best performance.

To configure load balancing

See "Advanced tab field descriptions" on page 175.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Advanced tab, under Load Balancing, in the WAN 1 Load text box, type the percentage of traffic to pass through WAN 1.

3 Click **Save**.

SMTP binding

Use SMTP binding when you have two different Internet connections with different ISPs used over different WAN ports. It ensures that email sent by a client goes over the WAN port associated with your email server.

If the SMTP server is on the same subnet as one of the WAN ports, the security gateway automatically binds the SMTP server to that WAN port, and you do not have to specify the bind information.

To configure SMTP binding

See "Advanced tab field descriptions" on page 175.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Advanced tab, under Load Balancing, in the Bind SMTP with WAN Port drop-down list, select a binding option.
3. Under DNS Gateway, click **Save**.

Binding to other protocols

You can use the routing functionality of the firewall to bind other traffic. You add a a static route to route traffic for the IP address of the destination server to a specific WAN port.

See "Configuring routing" on page 48.

Failover

You can configure the appliance to periodically test the connectivity to ensure that your connection is available to your clients. After the amount of time that you specify (for example, 10 seconds), the appliance issues a PING command to the URL you specify as the Alive Indicator. If you do not specify an Alive Indicator, the default gateway is used.

Note: When selecting a URL to check, choose a DNS name or IP address that you are sure will respond to a request, or you may receive a false positive when the connection is actually available.

When the WAN port on model 320 fails, the security gateway fails over to the serial port, which is connected to a modem. On model 360 or 360R, if one of the WAN ports fails, the security gateway fails over to the other WAN port. If both WAN ports fail, the security gateway fails over to the serial port.

If a line is physically disconnected, then the line is considered disconnected and the appliance attempts to route traffic to the serial port or the other WAN port.

If the cable is not physically disconnected, the appliance performs line checking every few seconds to determine if a line is active. If the line fails, it is shown as disconnected on the Logging/Monitoring > Status tab and an alternate route for traffic is attempted.

See "Dial-up accounts" on page 39 to configure failover for a dial-up account.
See "Connecting manually to your PPPoE account" on page 34 to configure a echo request for accounts that use PPP.

To configure failover

See "Main Setup tab field descriptions" on page 164.

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. To configure an alive indicator for WAN1, on the Main Setup tab, under WAN1 (External), in the Alive Indicator Server text box, type the IP address or DNS-resolvable name of a server to which to send packets.
3. To configure an alive indicator for WAN2, on the Main Setup tab, under WAN2 (External), in the Alive Indicator Server text box, type the IP address or DNS-resolvable name of a server to which to send packets.
4. Click **Save**.

DNS gateway

You can specify a DNS gateway for local and remote name resolution over your VPN. For local and remote name resolution over VPN (Gateway-to-Gateway or Client-to-Gateway), the appliance can use a DNS gateway.

A backup DNS gateway can be specified. The DNS gateway handles name resolution, but should it become unavailable, the backup (generally a DNS gateway through your ISP) can take over.

To configure a DNS gateway

You can configure a primary and backup DNS gateway.

See "Advanced tab field descriptions" on page 175.

To configure a DNS gateway

1. In the SGMI, in the left pane, click **WAN/ISP**.
2. On the Advanced tab, under DNS Gateway, in the DNS Gateway text boxes, type the IP address of the DNS gateway.

3 Click **Save**.

To configure DNS gateway backup

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 On the Advanced tab, under DNS Gateway, check **Enable DNS Gateway Backup**.

3 Click **Save**.

Optional network settings

Optional network settings identify your appliance to the rest of your network. If you plan to connect to or refer to your appliance by name, you must configure these settings.

Some ISPs authenticate by the physical (MAC) address of your Ethernet port. This is common with broadband cable (DHCP) services. You can clone your computer's adapter address to connect to your ISP with the Symantec Gateway Security 300 Series. This is called MAC cloning or masking.

If the appliance is going to be a wireless access point, the optional network settings must be set. See *Symantec Gateway Security 300 Series Wireless Implementation Guide*.

For model 320, you configure the settings for the WAN port. For model 360 or 360R, you can configure the network settings for one or both WAN ports.

Before you configure optional network settings, gather the following information:

Host name	Name of the appliance. For example, marketing.
Domain name	Name by which you address the appliance over the Internet. For example, mysite.com. If the host name is marketing, the appliance would be marketing.mysite.com.
MAC address	Physical address of the WAN of the appliance. If you are performing MAC cloning, get the MAC address that your ISP is expecting to see rather than the address of the appliance.

To configure optional network settings

See "Advanced tab field descriptions" on page 175.

1 In the SGMI, in the left pane, click **WAN/ISP**.

2 For model 320, do the following:

- In the right pane, on the Main Setup tab, under Optional Network Settings, in the Host Name text box, type a host name.
  The host and domain names are case-sensitive.
- In the Domain Name text box, type domain name for the appliance.
- In the MAC Address text boxes, type the WAN network adapter address (MAC) that you are cloning.

3 For model 360 and 360R, do the following:

- To configure WAN1 or WAN 2, in the right pane, on the Main Setup tab, under Optional Network Settings, under WAN1 (External) or WAN 2 (External), do the following:

Host Name text box	Type a host name. The host and domain names are case-sensitive.
Domain Name text box	Type a domain name for the appliance
MAC Address text boxes	Type the WAN network adapter address (MAC) you are cloning.

4 Click **Save**.

After you click Save, the appliance restarts. Network connectivity is interrupted.

Chapter 4

Configuring internal connections

This chapter includes the following topics:

- Configuring LAN IP settings
- Configuring the appliance as DHCP server
- Configuring port assignments

LAN settings let you configure your Symantec Gateway Security 300 Series appliance to work in a new or existing internal network.

Each appliance is assigned an IP address and netmask by default. You can change this IP address and netmask. This way, you can specify an IP address and netmask for the appliance that fits your existing network.

You can also configure the appliance to work as a DHCP server for your LAN clients. This assigns IP addresses to the clients dynamically so that you do not have to configure each client to use a static IP address.

Note: Model 320 has four LAN ports. Models 360 and 360R have eight LAN ports. For each port, you must specify the port settings using the port assignments. These settings are used to configure secure wireless and wired LANs.

Configuring LAN IP settings

Each appliance has a default IP address of 192.168.0.1 with a default network mask of 255.255.255.0. You can configure the appliance to use a different IP address and netmask for the LAN. This is useful if you want to configure a LAN to use a unique subnet for your network environment. For example, if your

network already uses 192.168.0.x, you can change the appliance's IP address to 10.10.10.x, so you do not have to reconfigure your existing network.

You can change the appliance's IP address and netmask at any time. The default IP address is 192.168.0.1 and the default netmask is 255.255.255.0. Ensure that the IP address you choose for the appliance does not have zero (0) as the last octet.

You cannot set the appliance IP address to 192.168.1.0.

Warning: After you change the appliance's LAN IP address, you must browse to the new appliance IP address to use the SGMI. If you click the Back button in the browser, it attempts to access the old IP address.

To change the appliance LAN IP address

See "LAN IP & DHCP tab field descriptions" on page 161.

1. In the SGMI, in the left pane, click **LAN**.
2. In the right pane, on the LAN IP & DHCP tab, under Unit LAN IP, in the IP Address text boxes, type the new IP address.
3. In the Network Mask text box, type the new network mask.
4. Click **Save**.

Configuring the appliance as DHCP server

Dynamic Host Configuration Protocol (DHCP) allocates local IP addresses to computers on the LAN without manually assigning each computer its own IP address. This eliminates the need to have a static (permanent) IP address for each computer on the LAN and is useful if you have a limited number of IP addresses available. Each time a computer connected to the LAN is turned on, DHCP assigns it an IP address from the range of available addresses.

Note: Each client computer that you want to use DHCP must have its network configuration set to obtain its IP address automatically.

By default, the range of IP addresses that the appliance can assign is from 192.168.0.2 to 192.168.0.XXX, where XXX is the number of clients to support, plus two. For example, if you support 50 clients on your appliance, the last IP address in the range is 192.168.0.52. The DHCP server on the appliance serves IP addresses to up to 253 computers connected to it. If you change the IP address of

the appliance, adjust the DHCP IP address range appropriately. See "To change the DHCP IP address range" on page 60.

Table 4-1 shows the default start and end IP addresses for each model. The default range is based on the recommended number of concurrent clients for each model. The number of clients you can support may vary depending on your traffic characteristics.

Table 4-1 Default DHCP IP address ranges

Model	Number of Clients	Start IP Address	End IP Address
320	50	192.168.0.2	192.168.0.76
360	75	192.168.0.2	192.168.0.76

The DHCP server only supports class C networks. Class C networks have addresses from 192.0.0.0 through 223.255.255.0. The network number is the first three octets, being from 192.0.0 through 223.255.255. Each class C network can have one octet worth of hosts.

You can place the appliance in any class network, but the DHCP server does not support this.

If you have a mix of clients that use DHCP and static IP addresses, the static IP addresses must be outside the range of DHCP IP addresses. Also, you may want to assign static IP addresses to some services. For example, if you have a Web server on your site, you want to assign it a static address.

The DHCP server in the appliance is enabled by default. If you disable the DHCP server, each client connecting to the LAN must be assigned an IP address that is in the range. If you enable the roaming on the appliance as a secondary wireless access point, the DHCP server is disabled.

To configure the appliance as a DHCP server

You can enable or disable DHCP, and you can set the range of IP addresses that the appliance allocates to the clients.

See "LAN IP & DHCP tab field descriptions" on page 161.

To enable or disable DHCP

1. In the SGMI, in the left pane, click **LAN**.
2. In the right pane, on the LAN IP & DHCP tab, under DHCP, do one of the following:
   - To enable the appliance as a DHCP server, check **Enable**.
   - To disable the appliance as a DHCP server, check **Disable**.

3 In the Range Start IP text boxes, type the first IP address.

4 In the End IP text boxes, type the last IP address.

5 Click **Save**.

To change the DHCP IP address range

1 In the SGMI, in the left pane, click **LAN**.

2 In the right pane, on the LAN IP & DHCP tab, under DHCP, do the following:

- In the Range Start IP text boxes, type the first IP address.
- In the End IP text boxes, type the last IP address.

3 Click **Save**.

Monitoring DHCP usage

The DHCP Table lists the addresses assigned to connected clients. You can view the host name, IP address, physical address, and status for each client. This table takes up to one hour to fully update after the appliance has been rebooted.

To view DHCP usage

See "LAN field descriptions" on page 160.

- In the SGMI, in the left pane, click **LAN**.

Configuring port assignments

Port assignments on the security gateway let you specify if the LAN port resides on a trusted or untrusted network. Trusted ports are for networks not using VPN authentication to connect to the LAN. Untrusted ports are for wireless or wired networks using VPN clients to connect to LAN resources.

You can connect many network devices to the LAN ports: routers, switches, client machines, or other Symantec Gateway Security 300 Series appliances. For these options, select the Standard port assignment. If you are connecting a Symantec Gateway Security 300 Series appliances configured as a wireless access point to a LAN port, you can secure the wireless connection using VPN technology. See the *Symantec Gateway Security 300 Series Wireless Implementation Guide*.

Once a port assignment is set, the untrusted ports enable and enforce encrypted VPN traffic, using global tunnels to the appliance or using IPsec pass-thru to WAN-side endpoints.

Standard port assignment

When LAN ports are designated as standard, the appliance acts as a typical switch: it forwards traffic based on MAC address and traffic does not reach the security gateway engine unless it was specifically designated for it.

This option does not support client VPN tunnels terminating at the LAN. When a LAN port is set to Standard, it is not considered part of the VLAN.

When you select Standard, VPN traffic is not enforced at the switch, that is, a trusted private network is assumed.

To configure port assignments

You can set a specific LAN port to use a port assignment, or you can restore the default port settings.

See "Port Assignment tab field descriptions" on page 162.

To configure a port assignment

1. In the SGMI, in the left pane, click **LAN**.
2. In the right pane, on the Port Assignment tab, under Physical LAN Ports, from the Port numbers drop-down list, select a port assignment.
3. Click **Save**.

The appliance reboots when the port settings are saved.

To restore port assignment default settings

1. In the SGMI, in the left pane, click **LAN**.
2. In the right pane, on the Port Assignment tab, under Physical LAN Ports, click **Restore Defaults**.

The appliance reboots when the port settings are saved.

Chapter 5

Network traffic control

This chapter includes the following topics:

- Planning network access
- Understanding computers and computer groups
- Defining inbound access
- Defining outbound access
- Configuring services
- Configuring special applications
- Configuring advanced options

The Symantec Gateway Security 300 Series appliance includes firewall technology that let you configure the firewall component to meet your security policy requirements. When configuring the firewall, identify all computers (nodes) to be protected on your network.

Note: This chapter uses the terms computers. A computer is defined as anything that has its own IP address; for example: a terminal server, network photocopier, desktop PC, laptop, server, print server, and so on.

Planning network access

Developing a security policy helps you identify what you need to configure. See the *Symantec Gateway Security 300 Series Installation Guide*.

Before configuring the security gateway, consider the following:

- Learn about computers and computer groups. See "Understanding computers and computer groups" on page 64.

- What kinds of users will be protected by the security gateway? Will all users have the same access and privileges?
- What types of services do you want to make available to internal users?
- What standard application services do you want to make available to external users?
- What types of special application services do you want to allow for external users and hosts?

Understanding computers and computer groups

Computers are all nodes behind the appliance. This includes permanent resident laptops on the LAN, application servers, and any host or printer. You configure the appliance to recognize the computer by its MAC (physical) address.

Computer groups let you create outbound rules and apply them to computers who should have the same access. Instead of creating a traffic rule for each individual computer in your network, you define computer groups, assign each computer to a computer group, and then create rules for the group.

By default, all computers are part of the Everyone group and have no restrictions on Internet use until they are assigned to another computer group which has traffic rules configured. You can create rules that apply to the Everyone group, or, for greater control, you can divide the computers into one of four computer groups, and then assign each group different rules. If a computer is not defined in the computers table, it belongs to the Everyone computer group.

Note: The appliance has five computer groups: Everyone, Group 1, Group 2, Group 3, and Group 4. You cannot add, delete, or rename computer groups.

Before you create inbound and outbound rules to govern traffic, perform the following tasks in this order:

- Define the computer groups.
  See "Defining computer group membership" on page 65.
- Define computers behind the appliance and assign them to computer groups.
  See "Defining computer group membership" on page 65.

Defining computer group membership

Configuring computers is the first step in configuring the firewall component of the appliance.

When creating your security policy, assign the largest group of hosts to the Everyone computer group to minimize the input and management of MAC addresses. By default, all hosts belong to the Everyone computer group until you configure them to one of the four other computer groups.

Review your security policy to determine how many computer groups you need (if any) and which users should be assigned to each computer group.

The Computers tab lets you identify each computer by typing its MAC address, assign a static IP address, assign it to a computer group, and bind it to a PPPoE session (if your ISP offers multiple PPPoE sessions). See "PPPoE" on page 31.

Note: To find the MAC address of a Microsoft Windows-based computer, at a DOS prompt, type ipconfig /all and look for the physical address.

On models 360 and 360R, you can restrict the computer to using only one of the WAN ports. This is useful if you have two broadband accounts, one on each WAN port, and you want a particular computer to use only one. This is useful for servers or applications that must always use a specific WAN IP address such as FTP. The default is disabled.

To configure computers

If you are using an ISP with PPPoE sessions, you bind a host to a session (WAN IP) on this tab.

To stop the configuration process, you can click Cancel at anytime while configuring computers. To clear all the information from the tab, you can click Clear Form at any time.

Checking Reserve Host ensures that the DHCP server always offers the defined IP address to the computer you are defining, or you can set this IP address as a static address on the computer.

See "Computers tab field descriptions" on page 177.

To configure a new computer

1. In the left pane, click **Firewall**.
2. On the Computers tab, in the Host Name text box, type a host name.
3. In the Adapter (MAC) Address text box, type the address of the host's network interface card (NIC).

4 If the computer is an application server to which you want to allow access to an inbound rule, or to reserve an IP address for a computer that is not an application server, under Application Server, check **Reserve Host**.
See "Defining inbound access" on page 68.

5 In the IP Address text box, type the IP address of the host.

6 Under Computer Group, on the Computer Group drop-down list, select a group for your host to join.
The computer group properties are defined on the Firewall > Computer Groups tab. See "Defining inbound access" on page 68.

7 Under Session Association, in the Bind with PPPoE Session drop-down list, select the session to bind to this host.
You must have a multi-session PPPoE account with your ISP if you want to bind a host to a PPPoE session. If you do not have an PPPoE account with your ISP, leave the Bind with PPPoE Session drop-down list at Session 1.

8 Click **Add.**

To verify that a host has been configured, you can check the Host List displayed at the bottom of the window. The fields in the list map to the fields entered when you configured the host.

Once you have finished adding computers to an computer group, you can configure the properties for each computer group.

To update an existing computer

1 In the left pane, click **Firewall**.

2 In the right pane, on the Computers tab, under Host Identity, in the Select Host drop-down list, select a host.

3 Make the changes to the computers fields.

4 Click **Update**.

The updated computer is displayed in the Host List.

To delete an existing computer

1 In the left pane, click **Firewall**.

2 In the right pane, on the Computers tab, under Host Identity, in the Select Host drop-down list, select a host.

3 Click **Delete**.

Defining computer groups

Computer groups are logical groups of network entities used for outbound rules. You must configure and bind all local hosts (nodes) to the computer group they are in by using the Computers tab. See "Defining computer group membership" on page 65.

You can configure the following properties for an computer group:

- Antivirus policy enforcement.
  See "How antivirus policy enforcement (AVpe) works" on page 104.
- Content filtering.
  See "Advanced network traffic control" on page 103.
- Access control.
  See "Defining inbound access" on page 68.

To define computer group properties

See "Computer Groups tab field descriptions" on page 179.

1. In the left pane, click **Firewall**.
2. In the right pane, on the Computer Groups tab, under Security Policy, on the Computer Group drop-down list, select the computer group you want to configure.
3. To enable AVpe, Under Antivirus Policy Enforcement, check **Enable AntiVirus Policy Enforcement.**
4. If you enabled AVpe, click one of the following:
   - Warn Only
   - Block Connections
5. Under Content Filtering, if you check **Enable Content Filtering**, you also need to select one of the following:
   - Use Allow List
   - Use Deny List
6. Under Access Control (Outbound Rules) select one of the following:
   - No restrictions
   - Block ALL outbound access
   - Use rules defined in Outbound Rules Screen.
     See "Defining outbound access" on page 69.
7. Click **Save**.

Defining inbound access

Inbound rules control the type of traffic flowing into application servers on your appliance-protected networks. The default state for inbound traffic is that all traffic is denied (automatically blocked) until you configure inbound rules for each kind of traffic you want to allow. If the inbound traffic contains a protocol or application that is not part of an enabled rule, the connection request is denied and logged. The appliance supports a maximum of 25 inbound rules.

When creating inbound rules, you must specify the applications server, the service, protocols, and ports that the rule allows, and source and destination information for each rule. When an inbound rule exists, any external host can successfully pass inbound traffic matching the rule.

Inbound rules redirect traffic that arrives on the WAN ports to another internal server on the protected LAN. For example, an inbound rule enabled for HTTP results in all HTTP traffic arriving on the WAN port to be redirected to the server specified as the HTTP application server. You must define the server before using it in a rule.

Inbound rules are not bound to a computer group.

To define inbound access

To stop the configuration process, click Cancel at any time while configuring computers.

To clear all the information from the tab, click Clear Form at any time.

See "Inbound Rules field descriptions" on page 180.

To define a new inbound rule

1. In the SGMI, in the left pane, click **Firewall**.
2. To create a new rule, in the right pane, on the Inbound Rules tab, under Rule Definition, in the Name text box, type a unique name for the inbound rule.
3. Check **Enable Rule**.
4. In the Application Server drop-down list, select a defined computer. Computers are defined on the Computers tab in the Firewall section.
5. On the Service drop-down list, select an inbound service.
6. Click **Add**.

The configured rule is displayed in the Inbound Rules List.

To update an existing inbound rule

1. In the left pane, click **Firewall**.

2 In the right pane, on the Inbound Rules tab, on the Rule drop-down list, select an existing inbound rule.

3 Click **Select**.

4 Make the changes to the inbound rules fields.

5 Click **Update**.

The configured rule is displayed in the Inbound Rules List.

To delete an inbound rule

1 In the left pane, click **Firewall**.

2 In the right pane, on the Inbound Rules tab, on the Rule drop-down list, select an existing inbound rule.

3 Click **Delete**.

Defining outbound access

By default, all computer groups are allowed outbound access. Also by default, all computers that you protect are in the Everyone computer group. When you define an outbound rule for a given computer group, and check the Use rules defined in Outbound Rules Screen checkbox, then all other traffic is blocked unless an outbound rule is defined to allow it. You must give each outbound rule a unique name.

You must also specify the type of traffic the rule allows. Outbound rules let you define traffic to permit, rather than specifying traffic to deny or block. Once an outbound rule is added to the computer group, all other traffic is denied unless there is a specific rule to let it pass.

The following list is the predefined outbound services:

- DNS
- FTP
- HTTP
- HTTPS
- Mail (SMTP)
- Mail (POP3)
- RADIUS Auth
- Telnet
- VPN IPSec

- VPN PPTP
- LiveUpdate
- SESA Server
- SESA Agent
- RealAudio1
- RealAudio2
- RealAudio 3
- PCA TCP
- PCA UDP
- TFTP
- SNMP

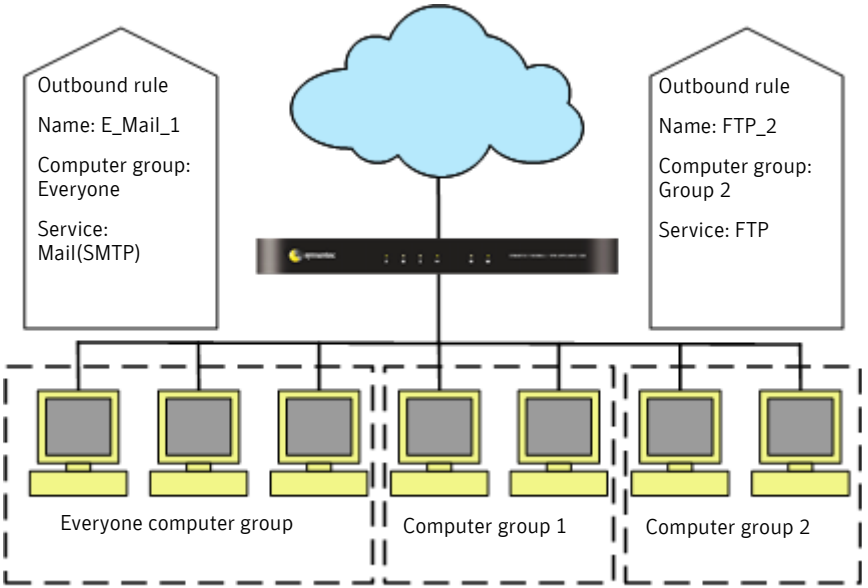
If you have services that are not on this list, or a service that does not use its default port, you can create your own custom services. You must create the custom services before creating the outbound rule.

See "Configuring services" on page 72.

An outbound rule enabled for FTP service for computer group 2 allows the members of computer group 2 outbound FTP service. An outbound rule enabled for Mail (SMTP) service for the Everyone computer group lets all members of the Everyone group to send outbound email. An outbound rule enabled for FTP service for computer group 2 would allow the members of group 2 outbound FTP

service. If computer group 1 has no rules, all outbound traffic is allowed by default. If Figure 5-1 shows a diagram of these examples.

Figure 5-1 Outbound rules example



To define outbound access

You can manage your outbound access by creating a rule, updating it when your needs change, or deleting it when you no longer need it. You can also temporarily disable outbound access for troubleshooting or controlling traffic.

See "Outbound Rules tab field descriptions" on page 181.

To define an outbound rule

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Outbound Rules tab, under Computer Groups, on the Computer Group drop-down list, select an computer group.
   To see a list of rules for the selected computer group, click **View**.
3. In the Name text box, type a unique name for the outbound rule.
4. Check **Enable Rule**.
5. On the Service drop-down list, select an outbound service.
6. Click **Add**.

The configured rule is displayed in the Outbound Rules List.

To update an existing outbound rule

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Outbound Rules tab, under Computer Groups, on the Computer Group drop-down list, select an computer group.
   To see a list of rules for the selected computer group, click **View**.
3. On the Rule drop-down list, select an existing outbound rule.
4. Make the changes to the outbound rules fields.
5. Click **Update**.
   The configured rule is displayed in the Outbound Rules List.

To delete an outbound rule

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Outbound Rules tab, under Computer Groups, on the Computer Group drop-down list, select an computer group.
   To see a list of rules for the selected computer group, click **View**.
3. In the right pane, on the Outbound Rules tab, on the Rule drop-down list, select an existing outbound rule.
4. Click **Delete**.

Configuring services

The Firewall > Services tab lets you define additional service applications, used in inbound rules and outbound rules for traffic to pass that are not already covered by the predefined services. You must configure these services before you can use them in any rules. The name of the service should identify the protocol or type of traffic that the rule allows.

You must specify the type of traffic and the destination server for that traffic. The type of traffic is selected from the list of predefined services and custom services.

Note: On models 360 and 360R, FTP application servers must be bound to a WAN port, WAN 1 or WAN 2. All other applications, such as HTTP, do not require binding to a WAN port. See "Binding to other protocols" on page 52.

There are two types of protocols used by services: TCP and UDP. The port range specifies which port filter can communicate on the appliance. For protocols that allow for a port range, you must specify the listen on port starting and ending

port number. For protocols that use a single port number, the listen on port starting and ending port number is the same.

Redirecting services

You can also configure services to be redirected from the ports they would normally enter (Listen on Port) to another port (Redirect to Port). Service redirection only applies to inbound rules. Outbound rules ignore this setting.

For example, to redirect inbound Web traffic entering on port 80 and using TCP protocol, to an internal Web server listening for TCP on port 8080, you would create a new service application called WEB_8080. Select TCP as the protocol, and type 80 for both the start and end Listen to Ports. For both the start and end Redirect To Ports, type 8080. Then create and enable an inbound rule for the Web application server that uses WEB_8080 as a service.

Note: Redirection port range sizes must be the same as the Listen on port ranges. For example, if the Listen on port range is 21 to 25, the redirection port range must also be four ports.

To redirect inbound traffic to the original destination port, leave the redirect fields blank.

To configure a service

Create a service before you add it to an inbound rule. Once you create a service, you can update or delete it.

See "Services tab field descriptions" on page 182.

To configure a service

1. In the SGMI, in the left pane, click **Firewall**.
2. Under Application Settings, in the Name text box, type a name for the service that represents the application.
3. In the Protocol drop-down list, select **TCP** or **UDP**.
4. In the Listen on Port(s): Start text box, type a port number.
5. In the Listen on Port(s): End text box, type a port number.
6. In the Redirect to Port(s): Start text box, type a port number.
   Redirect only applies to inbound rules. If you are creating a service for an outbound rule, leave the Redirect to Port(s) text boxes blank.
   To redirect inbound traffic to the original destination port, leave the Redirect text boxes blank.

7 In the Redirect to Port(s): End text box, type a port number.

8 Click **Add**.

To update an existing service

1 In the SGMI, in the left pane, click **Firewall**.

2 In the right pane, on the Services tab, on the Application drop-down list, select an existing service.

3 Make the changes to the services fields.

4 Click **Update**.

The configured Service is displayed in the Service List.

To delete a service

1 In the SGMI, in the left pane, click **Firewall**.

2 In the right pane, on the Services tab, on the Application drop-down list, select an existing service.

3 Click **Delete**.

Configuring special applications

Special applications are used for dynamic port forwarding. To determine what ports and protocols an application needs for operation, consult the application's documentation for information on firewall or NAT usage.

Some applications may need more than one entry defined and enabled; for example, when they have multiple port ranges in use. Special applications are global in scope and overwrites any computer group specific outbound rules or inbound rules. When enabled, the traffic specified can pass in either direction from any host.

Certain applications with two-way communication (such as games and video conferencing) need ports open in the firewall. Normally, you open ports with the Inbound Rules tab. But inbound rules only open ports for the application server IP address defined in its settings, because firewalls using NAT can only open a defined service for a single computer on the LAN (when using a single external IP).

The Special Applications tab works around this limitation by letting you set port triggers. The appliance listens for outgoing traffic on a range of ports from computers on the LAN and if it sees traffic, it opens an incoming port range for that computer. Once the communication is done, the appliance starts listening again so that another computer can trigger the ports to be opened for it.

Port triggers can be used very quickly (milliseconds), but for only one computer at a time. The speed with which port triggers are used gives the illusion of allowing multiple computers having the same ports opened.

Special Applications entries work best with applications that require low throughput. You may experience reduced performance with multiple computers activating streaming media or a heavy incoming or outgoing volume.

The appliance only listens for traffic on the LAN. The computer on the LAN activates the trigger, not traffic from the outside. The LAN application must initiate traffic and you must know the ports or range of ports it uses to set up a special applications entry. If traffic initiates from the outside, you must use an inbound rule.

To configure a special application

Special applications help with dynamic packet forwarding. Configure a special application for two-way communication. You can then edit it or delete it as your needs change.

See "Special Application tab field descriptions" on page 183.

To configure a special application

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Special Applications tab, under Select Applications, in the Name text box, type a name that represents the application.
3. Check **Enable**.
4. On the Outgoing Protocol drop-down list, select **TCP** or **UDP**.
5. In the Outgoing Port Range Start text box, type the first port number of the port range to listen on.
6. In the Outgoing Port Range End text box, type the last number of the port range to listen on.
7. In the Incoming Port Range Start text box, type the first port number in the range to open.
8. In the Incoming Port Range End text box, type the last port number in the range to open.
9. Click **Add**.

To update an existing special application

1. In the SGMI, in the left pane, click **Firewall**.

2 In the right pane, on the Special Application tab, on the Special Application drop-down list, select an existing special application.

3 Make the changes to the special applications fields.

4 Click **Update**.

The configured rule is displayed in the Special Application List.

To delete an special application

1 In the SGMI, in the left pane, click **Firewall**.

2 In the right pane, on the Special Applications tab, on the Application drop-down list, select an existing special application.

3 Click **Delete**.

Configuring advanced options

The Symantec Gateway Security 300 Series has several advanced firewall options for special circumstances.

Enabling the IDENT port

Queries to the IDENT port (113) normally result in the host name and company name information being returned. However, this service poses a security risk since attackers can use this information to hone in their attack methodology. By default, the appliance sets all ports to stealth mode. This configures a computer to appear invisible to those outside of the network. Some servers (like a certain email or MIRC servers) use the IDENT port of the system accessing them.

You can configure the appliance to enable the IDENT port. Enabling this setting makes port 113 closed (not open) and not stealth. You should enable this setting only if there are problems accessing a server (server time-outs).

Note: If you experience time-outs when using your mail (SMTP) service, enabling the IDENT port may correct this problem.

To enable the IDENT Port

See "Advanced tab field descriptions" on page 186.

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Advanced tab, under Optional Security Settings, check **Enable IDENT Port**.
3. Click **Save**.

Disabling NAT mode

You can configure the security gateway to work as a standard network router to separate different subnets on an internal network. Disabling NAT Mode disables the firewall security functions. This setting should only be used for Intranet deployments where the security gateway is used as a bridge on a protected network. When the security gateway is configured for NAT mode, it behaves as a 802.1D (MAC bridge) device.

To disable NAT Mode

See "Advanced tab field descriptions" on page 186.

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Advanced tab, under Optional Security Settings, check **Disable NAT Mode**.
3. Click **Save**.

Enabling IPsec pass-thru

IPsec pass-thru is supported by the security gateway. If the VPN client used in Exposed Host (DMZ) has problems connecting from behind the security gateway, use the None setting.

The following list includes the supported IPsec types:

- 1 SPI
  ADI - Assured Digital
- 2 SPI
  Standard (Symantec, Cisco Pix, and Nortel Contivity) clients
- 2 SPI-C
  Cisco Concentrator 30X0 Series clients

- Other
  Redcreek Ravlin
- None

Note: Only change the IPsec pass-thru setting if required to do so by Symantec Technical Support.

To configure IPsec pass-thru settings

See "Advanced tab field descriptions" on page 186.

1. In the SGMI, in the left pane, click **Firewall**.
2. On the Advanced tab, under IPsec Passthru Settings,
3. Click **Save**.

Configuring an exposed host

Exposed Host opens all ports so that one computer on a LAN has unrestricted two-way communication with Internet servers or users. This is useful for hosting games or special server applications.

All traffic that is not specifically allowed by inbound rules is directed to the exposed host.

Warning: Because of the security risk, only activate Exposed Host only when required to do so.

To configure an exposed host

See "Advanced tab field descriptions" on page 186.

1. In the left pane, click **Firewall**.
2. In the right pane, on the Advanced tab, under Exposed Host, check **Enable Exposed Host**.
3. In the LAN IP Address text boxes, type the IP address of the host you want to expose.
4. Click **Save**.

Managing ICMP requests

By default, the security gateway does not respond to external ICMP requests sent to the WAN ports. You can also configure the security gateway to block or allow ICMP requests on the WAN. LAN ICMP requests always respond.

To manage ICMP requests

See "Advanced tab field descriptions" on page 186.

1. In the SGMI, in the left pane, click **Firewall**.
2. In the right pane, on the Advanced tab, under Optional Security Settings, do one of the following:
3. To block ICMP requests, click **Enable**.
4. To allow ICMP requests, click **Disable**.
5. Click **Save**.

Chapter 6

Establishing secure VPN connections

This chapter includes the following topics:

- About using this chapter
- Creating security policies
- Identifying users
- Configuring Gateway-to-Gateway tunnels
- Configuring Client-to-Gateway VPN tunnels
- Monitoring VPN tunnel status

Virtual Private Networks (VPNs) let you securely extend the boundaries of your internal network and use insecure communication channels (such as the Internet) to safely transport sensitive data. VPNs are used to allow a single user or remote network to access the protected resources of another network.

Symantec Gateway Security 300 Series appliances support three types of VPN tunnels: Gateway-to-Gateway, Client-to-Gateway, and wireless Client-to-Gateway. To configure wireless Client-to-Gateway tunnels, see the *Symantec Gateway Security 300 Series Wireless Implementation Guide*.

Securing your network connections using VPN technology is an important step in ensuring the quality and integrity of your data. This section describes some key concepts and components you need to understand to effectively configure and use the appliance's VPN feature.

VPN tunnels can also support dynamic and static Gateway-to-Gateway configurations, where tunnel parameters are created at each security gateway. Both ends must have the same parameters, including secret keys, security parameter indexes (SPIs), authentication schemes, encryption methods.

About using this chapter

Each section begins with an explanation of the feature it is describing (such as what a VPN policy is, how it works, and how you use it). If you are an experienced network or IT administrator, you may want to proceed directly to the latter half of the section for configuration instructions.

If you do not have significant network or IT experience or have never configured a security gateway (Symantec or otherwise), you should read the first half of each section before configuring the feature.

At the end of "Configuring Gateway-to-Gateway tunnels" on page 88 and "Configuring Client-to-Gateway VPN tunnels" on page 96, there are worksheets for you to fill out with the information you entered so that you may easily share connection information with your clients and remote gateway administrators.

Creating security policies

The VPN tunnel establishment negotiation occurs in two phases. In Phase 1, the Internet Key Exchange (IKE) negotiation creates an IKE security association with its peer to protect Phase 2 of the negotiation, which determines the protocol security association for the tunnel. For Gateway-to-Gateway connections, either security gateway can initiate Phase 1 or Phase 2 renegotiation at any time. Either security gateway can also specify intervals after which to renegotiate. For Client-to-Gateway connections, only the client can initiate Phase 1 or Phase 2 renegotiation. Phase 2 renegotiation is referred to as quick mode renegotiation.

Note: Symantec Gateway Security 300 Series does not support VPN tunnel compression. To create a Gateway-to-Gateway tunnel between an Symantec Gateway Security 300 Series appliance and a remote Symantec Gateway Security 5400 Series appliance or Symantec Enterprise Firewall, set the compression to NONE on the remote gateway.

Understanding VPN policies

For each phase of negotiation, the appliance uses a policy, which is a predefined set of parameters. The appliance supports two types of security policies, Global IKE and VPN.

Global IKE Policy (Phase 1, non-configurable, except for SA lifetime parameter)

The security gateway includes a predefined global IKE policy that automatically applies to your IKE Phase 1 negotiations. This global IKE policy works in conjunction with the VPN policy you configure for Phase 2 negotiations. The Global IKE Policy provides the parameters that define Phase 1 negotiations of the IKE tunnel, while the VPN policy you configure and select provides the parameters for Phase 2 negotiations.

The only parameter in the Global IKE Policy whose setting can be changed is the SA (security association) Lifetime, which specifies the period of time after which the tunnel rekeys (in minutes). This parameter is located in VPN > Advanced > Global IKE Settings (Phase 1 Rekey).

When two security gateways are negotiating Phase 1, the first security gateway sends a list of proposals, called a transform proposal list. The security gateway to which it is connecting then selects a proposal from the list that it likes best, generally the strongest available option. You cannot change the transform proposal list on the appliance; however this information may be useful to give to the remote gateway administrator.Table 6-1 lists the order of the Symantec Gateway Security 300 IKE proposals.

Table 6-1 IKE proposal order

Data Privacy	Data Integrity	Diffie-Hellman
3DES	SHA1	Group 5
3DES	MD5	Group 5
3DES	SHA1	Group 2
3DES	MD5	Group 2
DES	SHA1	Group 1
DES	MD5	Group 1

Some settings are configurable at a global level for Client-to-Gateway tunnels. See “Setting global policy settings for Client-to-Gateway VPN tunnels” on page 101.

VPN Policies (Phase 2, configurable)

The security gateway includes a set of four pre-defined, configurable VPN policies that apply to Phase 2 tunnel negotiations. Rather than configuring data privacy, data integrity, and data compression algorithms for every tunnel you create, the security gateway lets you configure standard, reusable VPN policies

and then later associate them with multiple secure tunnels. You can select a pre-defined policy, or you can create your own using the VPN Policies tab.

VPN policies group together common characteristics for tunnels, and allow rapid setup of additional tunnels with the same characteristics. The security gateway also includes a handful of commonly used VPN policies, for both static and dynamic tunnels.

You can define more than one VPN policy, varying the components you select for each one. If you do this, ensure that your naming conventions let you distinguish between policies that use the same encapsulation mode. When you are ready to create your secure tunnels, clearly defined naming conventions will make selecting the correct VPN policy easier.

Note: You cannot delete pre-defined VPN policies.

Creating custom Phase 2 VPN policies

VPN Policies are pre-configured for typical VPN setups. If you require customized settings (for compatibility with 3rd party equipment, for example) then you can create a custom Phase 2 Policy on the VPN Policies tab.

A VPN policy groups together common characteristics for VPN tunnels. Rather than configuring data privacy, data integrity, and data compression algorithms for every tunnel that you create, you can configure standard, reusable VPN policies and apply them to multiple secure tunnels.

Note: Configuring a VPN policy is optional for dynamic tunnels.

To create a custom Phase 2 VPN policy

See "VPN Policies tab field descriptions" on page 200.

1. In the SGMI, in the left pane, click **VPN**.
2. In the right pane, on the VPN Policies tab, under IPsec Security Association (Phase 2) Parameters, in the Name text box, type a name for the VPN policy.
3. To edit an existing policy, from the VPN Policy drop-down list, select a VPN policy.
4. On the Data Integrity (Authentication) drop-down list, select an authentication.
5. On the Data Confidentiality (Encryption) drop-down list, select an encryption type.

6 In the SA Lifetime text box, type the number of minutes you want the security association to stay alive before a rekey occurs.
The VPN tunnel is temporarily interrupted when rekeys occur.

7 In the Data Volume Limit text box, type the number of kilobytes of traffic to allow before a rekey occurs.

8 In the Inactivity Timeout text box, type the number of minutes of inactivity before a rekey occurs.

9 To use Perfect Forward Secrecy, do the following:

- On the Perfect Forward Secrecy drop-down list, select a Diffie-Hellman group.
- Next to Perfect Forward Secrecy, click **Enable**.

10 Click **Add**.

Viewing VPN Policies List

The VPN Policies List section of the VPN Policies window displays a summary of each VPN Policy that is configured on the appliance. Table 6-2 defines each field in the VPN Policies List summary.

Table 6-2 VPN Policies List fields

Field	Description
Name	Displays the name of the VPN Policy.
Encryption Method	Displays the encryption method selected for the VPN Policy.
SA Lifetime	Displays the configured SA Lifetime setting.
Data Volume Limit	Displays the configured Data Volume Limit setting.
Inactivity Timeout	Displays the configured inactivity timeout setting.
PFS	Shows the Perfect Forward Secrecy setting.

Identifying users

The appliance lets you configure two types of clients that use VPN: users and users with extended authentication.

Understanding user types

Users authenticate directly with the security gateway when connecting through a VPN tunnel. Users are defined on the security gateway Client Users tab. Users with extended authentication are not defined on the security gateway; they are defined on a RADIUS authentication server. You must configure the appliance to support remote administration of users with extended authentication.

Dynamic users

Dynamic users are not defined on the appliance; rather, they use extended authentication with RADIUS to authenticate their tunnels. You define dynamic users on the RADIUS server.

When a dynamic user attempts to authenticate, the appliance looks for that user name in the defined users list.When it does not find the user there, the appliance then uses the shared secret that he has entered in the client software. This shared secret should match the secret on the Advanced screen for the security gateway to which he is connecting. The appliance then starts extended authentication and prompts him for whatever information the RADIUS server requires (such as a user name or password).The RADIUS server authenticates the user and returns the RADIUS group of the user to the security gateway. The security gateway checks that the group matches one of the client tunnels and that the group is allowed to connect to the WAN, LAN, or WLAN. If so, the user's tunnel is established.

Users

Users authenticate using a client ID (user name) and pre-shared key that you assign to them. They enter the user name and password in their client software, that information is sent when they attempt to create a VPN tunnel to the security gateway.

Users are defined on the appliance, and may also use extended authentication.

Defining users

Ensure that you obtain all the pertinent authentication information from your RADIUS administrator to pass on to your users with extended authentication.

To define users

Users must be defined on the appliance, and may also use extended authentication. Dynamic users must use extended authentication and are not defined on the appliance.

To configure users

See "Client Users tab field descriptions" on page 199.

1. In the SGMI, in the left pane, click **VPN**.
2. In the right pane, on the Client Users tab, under VPN User Identity, in the User Name text box, type the name of a new user.
3. To edit an existing user, in the User drop-down list, select a user.
4. Check **Enable**.
5. In the Pre-shared Key text box, type the pre-shared key.
6. From the VPN Group drop-down list, select a VPN group for the user to join.
7. Click **Add**.

To enable users with extended authentication

See "Advanced tab field descriptions" on page 203.

1. In the SGMI, in the left pane, click **VPN**.
2. On the Advanced tab, in the Dynamic VPN Client Settings section, do the following:
   - Check **Enable Dynamic VPN Client Tunnels**.
   - In the Pre-shared Key text box, type a key that your dynamic users will enter in their client software.
3. In the RADIUS Settings section, do the following:

Primary RADIUS Server	Type the IP address or fully qualified domain name of the RADIUS server.
Secondary RADIUS Server	Type the IP address or fully qualified domain name of the RADIUS server that the security gateway uses for authentication should the primary server become unavailable.
Authentication Port (UDP)	Type the port on the RADIUS server on which the RADIUS service runs.
Shared Secret or Key	Type the RADIUS server key.

4. Click **Save**.
5. On the Client Tunnels tab, in the VPN Group drop-down list select the VPN group to which the users that use extended authentication belong.
6. Under Extended User Authentication, do the following:
   - Check Enable Extended User Authentication.

- In the RADIUS Group Binding text box, type the name of the user's RADIUS group.
  The RADIUS group is assigned to the user on the RADIUS server. The RADIUS server must return the value that you type in the RADIUS Group Binding text box in the filterID attribute.

7 Click **Save**.

Viewing the User List

The User List section in the Client Users window displays a summary of each static user that is configured on the appliance. Table 6-3 defines each field in the summary.

Table 6-3 User list fields

Field	Description
User Name	User name entered for the static VPN user.
Enable	Indicates whether a particular user can establish VPN tunnels to the security gateway.
Pre-Shared Key	Displays the pre-shared key entered for the user.
VPN Group	Lists the VPN Groups for which a user is configured.

Configuring Gateway-to-Gateway tunnels

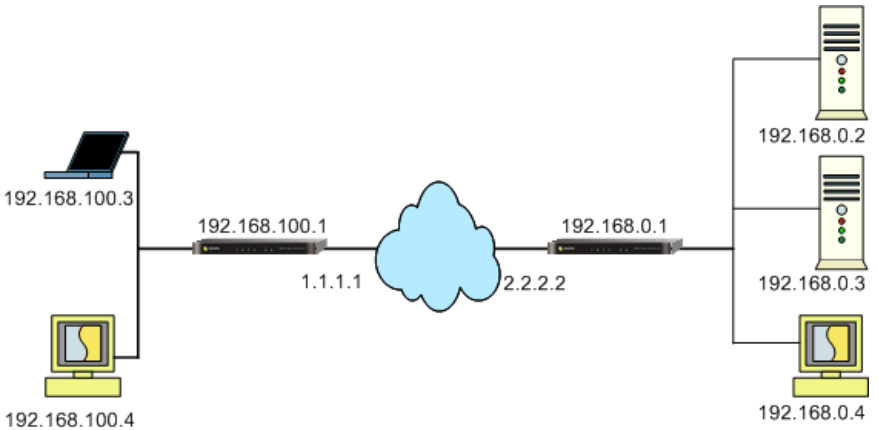
Gateway-to-Gateway tunnels help secure your internal network by providing a secure bridge to an external LAN. There are several tasks involved in successfully securing the network with Gateway-to-Gateway tunnels. The following section describes the Gateway-to-Gateway tunnels, and then provides procedures for configuring the tunnels.

Understanding Gateway-to-Gateway tunnels

You might want to make your network resources available to an outside group, such as another office of the company. Instead of requiring each user on the second network to establish their own, private secure connection, you can create one Gateway-to-Gateway tunnel, which makes resources on each network available to the other. This type of tunnel is LAN-to-LAN, instead of user-to-LAN.

The appliance supports Gateway-to-Gateway tunnel configurations. A Gateway-to-Gateway configuration is created when two security gateways are connected, through an internal network, or the Internet, from WAN port to WAN port.

Figure 6-1 Gateway-to-Gateway VPN tunnel configuration



This type of network configuration usually connects two subnets on the same network, or as shown in Figure 6-1, two remote offices through the Internet. Once a VPN tunnel is established, users protected by a security gateway at one site can establish a tunneled connection to the security gateway protecting the remotely located site. The remote user can connect to and access the resources of the private network as if the remote workstation was physically located inside the protected network.

The Symantec Gateway Security 300 Series can connect to another Symantec Gateway Security 300 Series appliance or to one of the following appliances:

- Symantec Gateway Security 5400 Series
- Symantec Firewall/VPN Appliance

Symantec Gateway Security 300 Series security gateways support creating a VPN tunnel to up to five remote subnets behind Symantec Enterprise Firewall or Symantec Gateway Security 5400 Series appliances, but not to another Symantec Gateway Security 300 Series appliance or Symantec Firewall/VPN Appliance. Tunnels between two Symantec Gateway Security 300 Series appliances are only made to the subnet on the LAN side of the appliance and only support the first set (subnet/mask) of the five sets of fields, which you define on the VPN > Dynamic Tunnels or VPN > Static Tunnels tabs.

If you have another (additional) subnet on the LAN side of the Symantec Gateway Security 300 Series security gateway, VPN client tunnels to the LAN side of the security gateway are not supported for computers on this separate subnet. Only computers residing on the appliance subnet (found on the LAN IP screen) are supported for LAN/WLAN-side VPN tunnels.

Note: Gateway-to-Gateway VPN tunnels are supported on the appliance's WAN ports; you cannot define Gateway-to-Gateway VPN tunnels on the appliance's LAN or WLAN ports.

Supported Gateway-to-Gateway VPN tunnels

The Symantec Gateway Security 300 Series appliance lets you configure two types of Gateway-to-Gateway VPN tunnels:

Dynamic	The security gateway comes with a predefined global IKE policy that automatically applies to your IKE Phase 1 negotiations. You can change the setting of the SA Lifetime parameter in the Global IKE Policy. SA Lifetime specifies the amount of time that the tunnel rekeys (in minutes). This parameter is located in VPN > Advanced > Global IKE Settings (Phase 1 Rekey).
Static	Static Gateway-to-Gateway configurations require you to manually enter tunnel parameters at each security gateway. Both ends must have the same parameters, including secret keys, security parameter indexes (SPIs), authentication schemes, encryption methods.

See "Configuring Gateway-to-Gateway tunnels" on page 88. See "Configuring static Gateway-to-Gateway tunnels" on page 93.

Gateway-to-gateway VPN tunnel persistence and high-availability

After the security gateway restarts, dynamic Gateway-to-Gateway VPN tunnels are re-established. Dynamic Gateway-to-Gateway VPN tunnels are also re-established if the WAN port status changes from disconnected to connected. This feature reduces management overhead by providing automatic reconnection of tunnels.

If the VPN tunnel fails to establish after three times, the security gateway waits between one and five minutes before attempting to reconnect. This process continues until the VPN tunnel is re-established.

If there is a network failure, the security gateway automatically re-establishes the VPN tunnel through a backup port (WAN port or serial port). If the IP

address of the security gateway changes, it re-establishes Gateway-to-Gateway VPN tunnels with the remote gateway using the new IP address.

Gateway-to-Gateway VPN tunnel interoperability

When Symantec Gateway Security 5400 Series or Symantec Enterprise Firewall initiates a Gateway-to-Gateway tunnel to a Symantec Gateway Security 300 Series appliance, it begins negotiation in Main Mode. The mode on the VPN tunnel definition on the Symantec Gateway Security 300 Series VPN tunnel definition must be Main Mode or the VPN tunnel will not establish.

Symantec Gateway Security 5400 Series and Symantec Enterprise Firewall accept either Main Mode or Aggressive Mode Phase 1 negotiations from a remote gateway. The Symantec Gateway Security 300 Series appliance can be configured for Main or Aggressive Mode. The default is Main Mode. When initiating a VPN tunnel to Symantec Gateway Security 5400 or Symantec Enterprise Firewall, configure the Symantec Gateway Security 300 Series appliance to use Main Mode so that if the remote end is the initiates the VPN tunnel, it does not establish a connection.

When a non-Symantec gateway initiates a VPN tunnel to an Symantec Gateway Security 300 Series appliance, the Symantec Gateway Security 300 Series appliance accepts the mode set by the administrator on the tunnel definition.

When a Symantec Gateway Security 300 Series appliance initiates a VPN tunnel to a non-Symantec security gateway, the Symantec Gateway Security 300 Series appliance should use the mode set by the administrator on the tunnel definition; the default setting is Main Mode. If Main Mode is not used, it may cause rekey problems if the remote security gateway tries to rekey first.

Creating VPN tunnels to Symantec Gateway Security 5400 Series clusters

To create a VPN tunnel to a Symantec Gateway Security 5400 Series appliance high-availability/load balancing cluster, define the VPN tunnel using the virtual IP address of the cluster. Tunnels between Symantec Gateway 300 Series and Symantec Gateway Security 5400 Series appliances are supported in high-availability only.

Configuring dynamic Gateway-to-Gateway tunnels

Dynamic tunnels, also known as IKE (Internet Key Exchange) tunnels, automatically generate authentication and encryption keys. Typically, a long password, called a pre-shared key (also known as a shared secret), is entered. The target security gateway must recognize this key for authentication to

succeed. If the key matches, then Security Parameter Index (SPI), authentication, and encryption keys are automatically generated and the tunnel is created. The security gateway usually re-keys (generates a new key) automatically at set intervals to ensure the continued integrity of the key.

Configuration tasks for dynamic Gateway-to-Gateway tunnels

Table 6-4 summarizes the tasks that are required to configure dynamic Gateway-to-Gateway VPN tunnels.

Note: Complete each step in Table 6-4 twice: first for the local security gateway and then for the remote security gateway.

Table 6-4 Dynamic Gateway-to-Gateway configuration tasks

Task	SGMI
Configure a VPN Policy (Phase 2 IKE negotiation). (Optional)	VPN > VPN Policies
Create a dynamic tunnel.	VPN > Dynamic Tunnels
Define IPsec Security Association Parameters. Select VPN Policy.	VPN > Dynamic Tunnels > IPsec Security Association
Define the local security gateway.	VPN > Dynamic Tunnels > Local Security Gateway
Define the remote security gateway.	VPN > Dynamic Tunnels > Remote Security Gateway
Repeat the above steps for the remote security gateway.	

To add a dynamic Gateway-to-Gateway tunnel

See "Dynamic Tunnels tab field descriptions" on page 189.

1. In the left pane, click **VPN**.
2. On the Dynamic Tunnels tab, in the Name text box, type a name for the new tunnel.
3. To edit an existing tunnel, from the VPN Tunnel drop-down list, select a VPN tunnel.
4. Check **Enable VPN Tunnel**.

5 On the VPN Policy drop-down list, select a VPN policy to which you want to bind to the tunnel.

6 If you have a multi-session PPPoE ISP account, under Local Security Gateway, in the PPPoE Session drop-down list, select a PPPoE session to which you want to bind to the tunnel.
If you do not have a multi-session PPPoE ISP account, skip this step.

7 For model 360 or 360R, on the Local Endpoint drop-down list, select an endpoint for the tunnel.

8 On the ID Type drop-down list, select a Phase 1 ID type.

9 In the Phase 1 ID text box, type the Phase 1 ID.

10 Under Remote Security Gateway, do the following:
- In the Gateway Address text box, type the remote gateway address.
- Optionally, in the ID Type drop-down list, select a Phase 1 ID type.
- Optionally, in the Phase 1 ID text box, type the Phase 1 ID.
- In the Pre-Shared Key text box, type a key.
- In each Remote Subnet IP text box, type the IP address of the destination network.
  To create a global tunnel, type 0.0.0.0.
- In each Mask text box, type the netmask of the destination network.
  To create a global tunnel, type 255.0.0.0.

11 Click **Add**.

Configuring static Gateway-to-Gateway tunnels

Static tunnels do not use any information from the Global IKE Policy (Phase 1 negotiation). You must manually type all of the information necessary to establish the tunnel. However, you can define a VPN Policy for Phase 2 negotiation.

When defining static tunnels, you must enter an authentication key, as well as an encryption key (if encryption is used). The keys must match on both sides of the VPN. In addition, a Security Parameter Index (SPI) is manually typed and included with every packet transmitted between security gateways. The SPI is a unique gateway identifier that indicates the set of keys that belongs to each packet.

Encryption and authentication key lengths

When you define a static tunnel, you must type an encryption key and an authentication key. Each key has a specific key length based on the method that

you chose. For each method, a key length is shown for both ASCII characters and Hex characters. Table 6-5 defines encryption key lengths.

Table 6-5 Encryption key lengths

Method	Key length in character bytes	Key length in Hex
DES	8	18 (0x + 16 hex digits)
3DES	24	50 (0x + 20 hex digits)
AES-128	16	18 (0x + 20 hex digits)
AES-192	24	50 (0x + 20 hex digits)
AES-256	32	66 (0x + 20 hex digits)

Table 6-6 defines authentication key lengths.

Table 6-6 Authentication key lengths

Method	Key length in character bytes	Key length in Hex
MD5	16	34 (0x + 16 hex digits)
SHA1	20	42 (0x + 20 hex digits)

Configuration tasks for static Gateway-to-Gateway tunnels

Table 6-7 describes the tasks that are required to configure a static Gateway-to-Gateway VPN tunnel.

Note: Complete each step in Table 6-7 twice: first for the local security gateway and then for the remote security gateway.

Table 6-7 Static Gateway-to-Gateway configuration tasks

Task	SGMI
Configure a VPN Policy (Phase 2 IKE negotiation). (Optional)	VPN > VPN Policies
Create a static tunnel	VPN > Static Tunnels
Define IPsec Security Association Parameters	VPN > Static Tunnels > IPsec Security Association

Table 6-7 Static Gateway-to-Gateway configuration tasks

Task	SGMI
Define the remote security gateway	VPN > Static Tunnels > Remote Security Gateway
Repeat the previous steps for the remote security gateway.	

To add a static Gateway-to-Gateway tunnel

See "Static Tunnels tab field descriptions" on page 193.

1. In the SGMI, in the left pane, click **VPN**.
2. In the right pane, on the Static Tunnels tab, under IPsec Security Association, in the Tunnel Name text box, type a name for the tunnel.
   To edit an existing static tunnel, on the VPN Tunnel drop-down list, select a VPN Tunnel.
3. Check **Enable VPN Tunnel**.
4. If you have a multi-session PPPoE ISP account, under Local Security Gateway, in the PPPoE Session drop-down list, select a PPPoE session to which you want to bind to the tunnel. If you do not have a multi-session PPPoE ISP account, skip this step.
5. For model 360 and 360R, on the Local Endpoint drop-down list, select the endpoint for the tunnel.
6. In the Incoming SPI text box, type the incoming SPI to match the remote SPI.
7. In the Outgoing SPI text box, type the outgoing SPI to match the local SPI from the remote side.
8. On the VPN Policy drop-down list, select a VPN policy to which you want to bind to the tunnel.
   Use an existing VPN policy or create a new one.
   See "Understanding VPN policies" on page 82.
9. In the Encryption Key text box, type the encryption key to match the chosen VPN policy.
   Entry length must match the chosen VPN policy.
10. In the Authentication Key text box, type the authentication key to match the chosen VPN policy.
11. Under Remote Security Gateway, in the Gateway Address text box, type the gateway address to be the gateway address of the Symantec Enterprise VPN.

12 Next to NetBIOS Broadcast, click **Disable**.

13 Next to Global Tunnel, click **Disable**.

14 In the Remote Subnet IP text boxes, type the IP address of the remote subnet to the destination network.
To create a global tunnel, type 0.0.0.0.

15 In the Mask text boxes, type the mask to the netmask of the destination network.
To create a global tunnel, type 255.0.0.0.

16 Click **Add**.

Sharing information with the remote gateway administrator

Table 6-8 lists the information you should provide to the administrator of the appliance to which you are creating a Gateway-to-Gateway tunnel.

Table 6-8 Information to give the remote gateway administrator

Information	Value
IP address	
Authentication key (Static tunnel)	
Encryption key (Static tunnel)	
SPI (Static tunnel)	
Pre-shared key	
Local subnet/mask	
VPN policy encryption method	
VPN policy authentication method	
(Optional) Local phase 1 ID	

Configuring Client-to-Gateway VPN tunnels

Client-to-Gateway VPN tunnels let remote users running the Symantec Client VPN software (or any IPsec-compliant VPN client software) to safely connect over the Internet to a network secured by a Symantec security gateway.

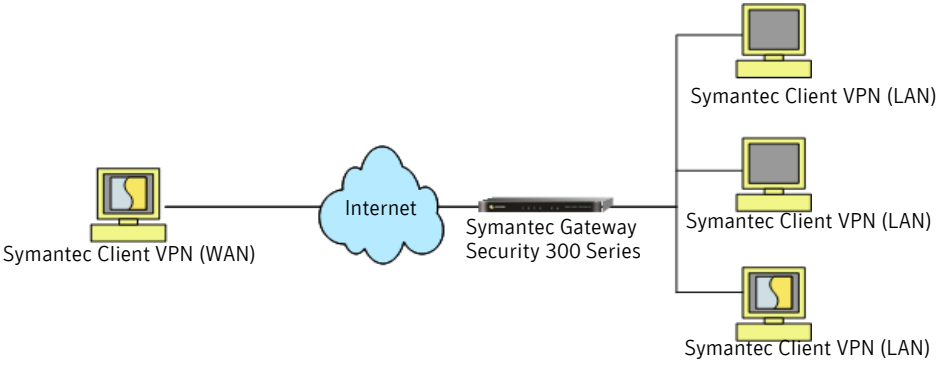
Understanding Client-to-Gateway VPN tunnels

Symantec Gateway Security 300 Series supports Client-to-Gateway VPN tunnel configurations. A Client-to-Gateway configuration is created when a workstation, running Symantec Client VPN software, connects to the security gateway from either inside the protected network or from a remote location through the Internet.

Note: Wireless clients can use client-to-gateway tunnels to secure their connections. See *Symantec Gateway Security 300 Series Wireless Implementation Guide*.

Once a VPN tunnel is established, remote users can connect to and safely access the resources of the private network, through the Internet, as if the remote workstation was physically located inside the protected network (see Figure 6-2).

Figure 6-2 Client-to-Gateway VPN tunnel configuration



In this diagram, there is a client that establishes a tunnel remotely (WAN) and three internal clients establishing a tunnel internally (LAN).

For each VPN group, you can define network settings to download to the client during Phase 1 configuration mode. The settings include the primary and secondary DNS servers, the WINS servers, and the primary domain controller. By pushing this information to the clients during configuration mode, each client will not have to configure that on his or her own, saving management time, and reducing the possibility of error.

For LAN-side VPN client tunnels, the only subnet that the client can access is the one defined on the LAN IP screen.

See "Configuring LAN IP settings" on page 57.

Symantec Client-to-Gateway VPN tunnels require a client ID and a shared key. You can also apply extended authentication using a RADIUS server to Client-to-Gateway VPN tunnels for additional authentication.

See "Defining users" on page 86.

You can configure two types of Client-to-Gateway users when configuring VPN tunnels: dynamic and static.

See "Identifying users" on page 85.

Understanding global tunnels

When a client establishes a VPN tunnel on the LAN, a global tunnel (0.0.0.0) is configured for the client. This forces all client traffic through the VPN tunnel terminating at the appliance. This is useful for untrusted networks, such as wireless, to keep traffic secure.

When establishing a tunnel on the WAN, the appliance's subnet (192.168.0.0 by default) is configured for the client allows a split tunnel so that the client can still access the Internet directly and only traffic destined for the LAN is sent through the VPN tunnel.

Configuration tasks for Client-to-Gateway VPN tunnels

Table 6-9 describes the tasks that are required to configure a Client-to-Gateway VPN tunnel.

Table 6-9 Client-to-Gateway VPN tunnel configuration tasks

Task	SGMI
Configure a VPN Policy (Phase 2 IKE negotiation). This is optional.	VPN > VPN Policies
Identify remote users.	VPN > Client Users > VPN User Identity
Enable client tunnel for selected VPN Group.	VPN > Client Tunnels > Group Tunnel Definition
Optionally, configure VPN network parameters (pushed to client during negotiations).	VPN > Client Tunnels > VPN Network Parameters

Table 6-9 Client-to-Gateway VPN tunnel configuration tasks

Task	SGMI
Optionally, configure RADIUS authentication.	VPN > Client Tunnels > Extended User Authentication VPN > Advanced > RADIUS Settings
Optionally, configure Antivirus Policy Enforcement.	VPN > Client Tunnels > Antivirus Policy
Select the VPN policy that applies to the tunnel.	VPN > Advanced > Global VPN Client Settings

Defining client VPN tunnels

This section describes how to define client VPN tunnels. Defining client VPN tunnels consists of the following tasks:

- Enabling client tunnels for selected VPN groups for WAN connections and/or LAN/WLAN connections
- Configuring VPN network parameters that are pushed to the Client VPN during tunnel negotiations (optional)
- Configuring RADIUS authentication (optional)
- Configuring antivirus policy enforcement (optional)
- Configuring content filtering (optional)
  If you enable content filtering for remote WAN-side VPN clients, you must have DNS servers on the local LAN. In Symantec Client VPN version 8.0, you can define two different tunnels: one for WAN which uses the domain name, and one for LAN, which uses the IP address. Then, put those tunnels in a gateway group. This way, when you create the tunnel, if the first tunnel fails (because the name cannot be resolved, for example) the IP address can be used to connect.
  See *Symantec Client VPN User's Guide*.

To define client tunnels

See "Client Tunnels tab field descriptions" on page 197.

1. In the SGMI, in the left pane, click **VPN**.
2. In the right pane, on the Client Tunnels tab, under Group Tunnel Definition, in the VPN Group drop-down list, select a VPN group.
3. To enable client VPNs for the chosen VPN Group on WAN or WLAN/LAN connections, click one or both of the following:

- Enable client VPNs on WAN side
- Enable client VPNs on WLAN/LAN side

4 Optionally, under VPN Network Parameters, in the Primary DNS text box, type the name of the primary DNS server.

5 Optionally, in the Secondary DNS text box, type the name of the secondary DNS server.
Domain Name System or Service (DNS) is an Internet service that translates domain names into IP addresses.

6 Optionally, in the Primary WINS text box, type the name of the primary WINS server.
This is an optional step.Windows Internet Naming Service (WINS) is a system that determines the IP address associated with a particular network computer.

7 Optionally, in the Secondary WINS text box, type the name of the secondary WINS server.

8 Optionally, in the Primary Domain Controller text box, type the name of the primary domain controller.

9 (Optional) Under Extended User Authentication, check **Enable Extended User Authentication**.

10 (Optional) In the RADIUS Group Binding text box, type the RADIUS Group Binding name.
The RADIUS Group Binding name must match the filter ID parameter returned from the RADIUS server.

11 To enable AVpe, under WAN Client Policy, do the following:

- Check **Enable Antivirus Policy Enforcement**.
- To log a warning to the Symantec Gateway Security log that a user is connecting that is not compliant with AVpe policy, click **Warn Only**.
- To stop the user's traffic if they are not compliant with the AVpe policy, click **Block Connections**.

12 To enable content filtering, under WAN Client Policy, do the following:

- Check **Enable Content Filtering**.
- To permit traffic and block other traffic, click **Use Allow List**.
- To block traffic and permit other traffic, click **Use Deny List**.

13 Click **Update**.

Setting global policy settings for Client-to-Gateway VPN tunnels

Some settings are configurable at a global level for Client-to-Gateway VPN tunnels. These settings configure the Phase 1 ID type for all client VPN tunnels connecting to the security gateway.

These settings are shared by all three VPN groups.

To set global policy settings for Client-to-Gateway VPN tunnels

See "Advanced tab field descriptions" on page 203.

1. In the SGMI, in the left pane, click **VPN**.
2. In the right pane, on the Advanced tab, under Global VPN Client Settings, do the following:
   - On the Local Gateway Phase 1 ID Type drop-down list, select an ID type.
   - In the Local Gateway Phase 1 ID text box, type the value that corresponds to the ID type you selected.
   - On the VPN Policy drop-down list, select a VPN policy to apply to all client tunnels.
3. Under Dynamic VPN Client Settings, do the following:
   - To enable dynamic users for all three VPN groups, click **Enable Dynamic VPN Client Tunnels**.
   - In the Pre-shared Key text box, type a string of characters for the key.
4. Click **Save**.

Sharing information with your clients

After you have configured the Client-to-Gateway VPN tunnel, you must disseminate the gateway information to your clients so that they may connect to it. Use Table 6-10 to record information to give your clients so that they may connect to the security gateway.

Table 6-10 Information to give clients

Information	Value
Gateway IP address or fully qualified domain name	
Pre-shared key (user)	Share this information only verbally or by other secure means.
Client ID	

Table 6-10 Information to give clients

Information	Value
RADIUS user name (Optional)	
RADIUS shared secret (user with extended authentication) (Optional)	
Phase 1 ID (Optional)	

Monitoring VPN tunnel status

The VPN Status window lets you view the status for each configured dynamic and static Gateway-to-Gateway VPN tunnel. The status for static tunnels is either Enabled or Disabled; the status for dynamic tunnels is Connected, Enabled, or Disabled. The status for static tunnels is never connected because there is no negotiation for static tunnels.

The information on the Status window is current when you select it. Conditions may change while you are viewing the screen. Refresh displays the most current conditions.

To monitor VPN tunnel status

You can monitor tunnel status by verifying both ends of the tunnel, and by monitoring the Status window.

See "Status tab field descriptions" on page 202.

To verify that the tunnel is operational on both ends

- From a local host, issue a PING command to a computer on the remote network.

To refresh the information on the Status window

1. In the SGMI, in the left pane, click **VPN**.
2. In the right pane, on the Status tab, on the bottom of the Status window, click **Refresh**.

Chapter 7

Advanced network traffic control

This chapter includes the following topics:

- How antivirus policy enforcement (AVpe) works
- Before you begin configuring AVpe
- Configuring AVpe
- Monitoring antivirus status
- Verifying AVpe operation
- About content filtering
- Managing content filtering lists
- Monitoring content filtering

Advanced network traffic control features of the Symantec Gateway Security 300 Series appliance include antivirus policy enforcement (AVpe) and content filtering.

AVpe lets you monitor client antivirus configurations and, if necessary, enforce security policies to restrict network access to only those clients who are protected by antivirus software with the virus definitions defined by the policy master.

The appliance also supports basic content filtering for outbound traffic. You use content filtering to restrict the URLs to which clients have access. For example, to restrict your users from seeing gambling sites, you configure content filtering to deny access to gambling URLs that you specify.

How antivirus policy enforcement (AVpe) works

AVpe monitors the AV configuration of supported Symantec connected policy masters and client workstations attempting to gain access to your corporate network. See the Symantec Gateway Security 300 Series Release Notes for the version of the product you are using to determine the supported AV products and how their configuration and usage differs from the following information.

AVpe works in two different environments: a network with an internal Symantec AntiVirus Corporate Edition server that maintains antivirus information or a network of clients that are unmanaged.

If your network has an internal Symantec AntiVirus Corporate Edition server, when you configure AVpe, you designate a primary and (optionally) a secondary antivirus server that is accessible to your network through LAN or WAN connections. If your network has clients that are unmanaged, you designate one client as master, and all other clients verify their versions against the master.

The first time an internal client requests a DHCP connection, attempts an external connection, or any time a client initiates a VPN tunnel (originating from your LAN or remotely through the Internet), the appliance retrieves the client's antivirus policy configuration and compares it against the current antivirus policy requirements. If the client is not in compliance, the traffic is warned or blocked (as indicated when you configure AVpe) and a message is logged.

You can configure the appliance to monitor client or server configurations at specified intervals (the default setting is every 10 minutes). Once a client is connected, the appliance rechecks the client's antivirus compliance at user-defined intervals. After the specified interval (the default interval is eight hours), clients are re-queried to check for compliance. If the AV policy master shows updates were made, the clients are allowed an eight-hour grace period (the default LiveUpdate interval on unmanaged clients) where they will still be compliant if they have the last AV policy master definition version. After this period, the clients will be considered non-compliant with the AV policy.

Table 7-1 describes client compliance and the subsequent actions taken.

Table 7-1 Client compliance actions

If the client is	Then
Compliant with current antivirus policies	Client is granted access to the firewall.
Antivirus protection is out-of-date	The connection is allowed to pass, but the appliance logs a warning or completely blocks access, depending on the option you select.

Clients who have been denied access can still connect to Symantec AntiVirus Corporate Edition or Symantec LiveUpdate servers to update their virus definitions.

You determine whether to enforce antivirus compliance for local clients using computer groups. All local clients belong to computer groups. For each computer group, you enable or disable AVpe. The default AVpe status for all computer groups is disabled. See "Understanding computers and computer groups" on page 64.

If content filtering and antivirus policy enforcement are enabled at the same time, content filtering takes precedence over antivirus policy enforcement processing for outbound traffic only. If a content filtering violation occurs and a client is blocked from viewing content, a message is logged and no antivirus policy enforcement rules are processed.

AVpe is supported for outbound connections and VPN client connections only.

Note: You must place UNIX/Linux clients or clients with a non-supported AV client in a computer group without AVpe.

Before you begin configuring AVpe

Before configuring the Symantec Gateway Security 300 Series appliance, make sure you do the following:

- Include your AVpe needs in your strategy for group assignments. AVpe is supported for outbound connections and VPN client connections only. Determine those clients whose virus definitions will be checked and those (if any) who will be allowed conditional or unconditional network access. Then assign users to the appropriate access or VPN groups and select whether you will warn or block non-compliant clients who attempt to access the local network.

  Note: You must place UNIX/Linux clients or clients with a non-supported AV client in a computer group without AVpe.

  See "Defining computer groups" on page 67 or "Viewing the User List" on page 88.

- If you plan to use Symantec AntiVirus Corporate Edition servers, obtain the name of the primary and (optionally) the secondary servers used in your network.

- If your network is comprised of clients that are unmanaged and access LiveUpdate directly for their AV updates, decide which client to designate as the master. The master should always be turned on, have an active Symantec antivirus client, and have a connection to the Internet where it can download virus definition updates.
- If your network topology includes a configuration in which client workstations are located behind an enclave firewall, and iff the firewall performs address transforms, which changes the client's actual IP address, the security gateway is unable to communicate with the client (as is required to validate client virus definitions). In this configuration, the security gateway contacts the firewall, not the client.
- Ensure that traffic is not being blocked by a personal firewall. You must allow UDP/Port 2967 on all personal firewalls. This is set by default in Symantec Client VPN version 8.0.

Configuring AVpe

Configuring AVpe for a Symantec AntiVirus Corporate Edition environment and a client-only network is similar.

Configuring for Symantec AntiVirus Corporate Edition servers involves the following tasks:

- Defining the location of the primary and (optionally) a secondary Symantec AntiVirus server and verifying that a client has the Symantec AntiVirus Corporate Edition client installed and that the virus definitions and the scanning engine on client computers are up-to-date.
  See "Configuring AVpe" on page 106.
- Enabling AVpe for Computer or VPN Groups.
  See "Enabling AVpe" on page 107.

Configuring for networks with unmanaged antivirus clients (without Symantec AntiVirus Corporate Edition) involves the following tasks:

- Defining the location of the policy master client and verifying that it has a supported Symantec antivirus client installed and that the virus definitions and the scanning engine on client computers are up-to-date.
- Enabling AVpe for Computer or VPN Groups.
  See "Enabling AVpe" on page 107.
- Configuring the AV clients.
  See "Configuring the antivirus clients" on page 109.

To configure antivirus policy enforcement

See "AVpe field descriptions" on page 207.

1. In the SGMI, in the left pane, click **Antivirus Policy**.
2. In the Primary AV Master text box, in the right pane, under Server Location, type the IP address or fully qualified domain name of your primary antivirus server or master client.
3. Optionally, in the Secondary AV Master text box, type the IP address or fully qualified domain name of a backup antivirus server, if supported in your environment.
4. In the Query AV Master Every text box, type an interval (in minutes) for the appliance to query the antivirus server for updated virus definitions.
5. To force a manual update, click **Query Master**.
6. Under Policy Validation, next to Verify AV Client is Active, select one of the following:
   - Latest Product Engine
     To check a client's antivirus configuration to ensure it uses a supported Symantec antivirus product with the latest product scan engine.
   - Any Version
     To check a client's antivirus configuration to verify that a the correct version of a supported Symantec antivirus product is installed on the client's workstation.
7. To enable the appliance to validate whether a client is using the latest virus definitions, check **Verify Latest Virus Definitions**.
8. In the Query Clients Every text box, type an interval (in minutes) for the appliance to query clients to validate whether they are using updated virus definitions.
9. Click **Save**.

Enabling AVpe

AVpe is enforced at the computer group and VPN group level. To enable AVpe, you first select a group, and then enable AVpe once for all members of that group. You also decide whether you want to warn or to denny WAN access to clients if their antivirus configuration is not compliant with expected security policies.

To enable AVpe

After you have configured AVpe, you must enable it for each computer or VPN group.

Note: Enabling AVpe for VPN groups is for WAN clients only. You enable AVpe for LAN VPN clients through Computer groups in the Firewall section.

See "Defining computer group membership" on page 65. See "Defining client VPN tunnels" on page 99.

See "Computer Groups tab field descriptions" on page 179.

See "Client Tunnels tab field descriptions" on page 197.

To enable antivirus policy enforcement for computer groups

1. In the SGMI, in the left pane, click **Firewall**.
2. On the Computer Groups tab, under Security Policy, on the Computer Group drop-down list, select the computer group for which you want to enable AVpe.
3. Under Antivirus Policy Enforcement, check **Enable Antivirus Policy Enforcement**, and then do one of the following:
   - To log warnings for clients with out-of-date virus definitions, click **Warn Only**.
   - To completely block connections from clients with out-of-date virus definitions, click **Block Connections**.
4. Click **Save**.
5. Repeat steps 2 through 6 to enable AVpe for each computer group.

To enable antivirus policy enforcement for VPN groups

1. In the left pane of the Security Gateway Management Interface (SGMI), click **VPN**.
2. On the Client Tunnels tab, under Group Tunnel Definition, on the VPN Group drop-down list, select the VPN group for which you want to enable AVpe.
3. Under WAN Client Policy, check **Enable Antivirus Policy Enforcement**, and then do one of the following:
   - To log warnings for clients with out-of-date virus definitions, click **Warn Only**.
   - To completely block connections from clients with out-of-date virus definitions, click **Block Connections**.

4 Click **Save**.

5 Repeat steps 2 through 6 to enable AVpe for each desired VPN group.

Configuring the antivirus clients

If the clients on your network are unmanaged and use LiveUpdate to install current virus definitions and engines, you must configure each client before it can be validated using AVpe. Each client that you want to validate with AVpe must have a supported Symantec antivirus product installed in unmanaged mode.

When you uninstall the client software, the registry keys that are created by this procedure are also removed.

Warning: Do not use this procedure for clients managed by a Symantec AntiVirus server.

To configure the AV clients

1 Install or configure each client's supported Symantec antivirus product in unmanaged mode.

2 Insert the Symantec Gateway Security 300 Series CD-ROM into the CD-ROM drive on a client computer.

3 In the Tools folder, copy SGS300_AVpe_client_Activation.reg to the client's desktop.

4 Double-click the file.

5 Repeat steps 2-4 for each client that you want to be validated using AVpe.

Monitoring antivirus status

The AV Master Status and Client Status sections of the AVpe tab lets you obtain an operational status of the primary and secondary antivirus master and clients configured in your network.

Any changes you make to the configuration of the primary or secondary antivirus server, once saved, are reflected in the AV Master Status field.

Log messages

When you enable AVpe and a client connection is denied (either because it is blocked or warned), a message is logged. You can view these log messages periodically to monitor your traffic.

To view AVpe log messages

See "View Log tab field descriptions" on page 154.

1. In the left pane of the Security Gateway Management Interface (SGMI), click **Logging/Monitoring**.
2. On the View Log tab, click **Refresh**.

Verifying AVpe operation

After you have enabled AVpe, you can test its operation by disabling Symantec AntiVirus Corporate Edition in a client workstation and then attempting to connect to the local network. If antivirus policy enforcement is properly configured, in the absence of enabled Symantec antivirus software, all connection attempts should be blocked or warned.

The status of the secondary antivirus server is not displayed unless the primary server is unreachable.

Note: The client workstation does not receive any notification that network access is blocked and a message is logged.

To test antivirus policy enforcement operation

See "Logging/Monitoring field descriptions" on page 151.

1. Uninstall Symantec AntiVirus Corporate Edition from a client workstation that has been configured as part of an computer group with AVpe enabled, with connections blocked.
2. Open a Web browser and attempt to connect to www.symantec.com.
   The connection attempt should fail and all communication through the firewall should be blocked.
3. From the left pane of the Security Gateway Management Interface (SGMI), click **Logging/Monitoring**.
4. Click **View Log** and check for a warning message indicating that all connection attempts for the particular client are blocked due to policy non-compliance.

If this message is present, then your AVpe feature is correctly configured and operational.

5 If you are able to connect to www.symantec.com, recheck your AVpe configuration settings and group assignments. Make sure that you uninstalled Symantec AntiVirus Corporate Edition from the client workstation, and that the client is a member of group with AVpe enabled, with connections blocked. Retry steps 1 through 4 above.

About content filtering

Symantec Gateway Security 300 Series supports basic content filtering for outbound traffic. You use content filtering to restrict the content to which clients have access. For example, to restrict your users from seeing gambling sites, you configure content filtering to deny access to gambling URLs that you specify.

Content filtering is administered through computer groups and VPN groups. A computer group is a group of computers defined in the Firewall section to which you apply the same rules. Similarly, a VPN group is a group of VPN users defined in the VPN section to which you apply the same rules. When you define a computer group, you specify if the group uses a content filtering deny or allow list. Deny lists (black lists) block internal access to sites on the list and allows all others sites. Allow lists (white lists) permit internal access to sites on the list, and blocks access to all other sites.

Note: By default, content filtering is disabled for all computer groups.

The allow list permits traffic to pass to sites that exactly match entries in the list. The content filtering engine drops connection requests sent to a destination that do not match the entries in the list. If the allow list is empty, all traffic is blocked.

If the deny list is empty, traffic is not filtered. Once entries are added to the deny list, the content filtering engine drops connection requests sent to a destination that exactly matches an entry. Traffic that does not match an entry is allowed to pass.

Special considerations

When content filtering and AVpe are concurrently enabled, content filtering is performed first. If the content filtering results in a blocked connection, AVpe is not processed; only a content filtering message is logged.

If you make changes to content filtering on the appliance, clear the DNS and browser caches on the client machine. If a URL is accessed by a client, but then the content filtering settings change to deny access to that URL, the cache may be used and allow the client access to the URL. Refer to your operating system documentation for information on clearing DNS caches and your browser's documentation for clearing the browser cache.

If you enable content filtering for remote WAN-side VPN clients, you must have DNS servers on the local LAN.

Managing content filtering lists

When you create allow and deny lists, you provide the allowed or denied fully qualified domain names. The appliance filters traffic by checking DNS lookup requests. There must be an exact match on the destination for action (blocking or warning) to occur.

For wild card functionality, specify only the domain name in the allow or deny list for specific sites. For example, to allow traffic to any Symantec site, add symantec.com to the allow list. This allows traffic to liveupdate.symantec.com, www.symantec.com, fileshare.symantec.com, and so on.

Content filtering applies to all outbound traffic, not just HTTP (Web) traffic.

Special considerations

If a site or security gateway uses redirection to transfer users from one URL to another, you must include both URLs in the list. For example, www.disney.com redirects users to www.disney.go.com. To allow your users to view this Web site, you must specify both www.disney.com and www.disney.go.com in the allow list.

If a site brings in content from other sites, you must add both URLs to the list. For example, www.cnn.com uses content from www.cnn.net.

To manage allow and deny lists

By default, the allow and deny lists are empty. Each filtering list can hold up to 100 entries. Each entry can be up to 128 characters long.

See "Content filtering field descriptions" on page 210.

To add a URL to an allow or deny list

1 In the left pane, click **Content Filtering**.

2 Under Select List, next to List Type, select **Allow** or **Deny**.

3 In the Input URL text box, type the name of a site you want to add to the list. For example, yoursite.com or mysite.com/pictures/me.html.

4 Click **Add**.
Repeat the previous two steps until you have all your URLs added to the list.

5 Click **Save List**.

To remove a URL from an allow or deny list

1 In the left pane, click **Content Filtering**.

2 From the Delete URL drop-down list, select the URL that you want to delete.

3 Click **Delete Entry**.

4 Click **Save List**.

Enabling content filtering for LAN

After you have set up the allow or deny lists, you must enable content filtering for each computer group for which you want to filter traffic. See "Defining inbound access" on page 68.

To enable content filtering for a computer group

See "Computer Groups tab field descriptions" on page 179.

1 In the left pane, click **Firewall**.

2 On the Computer Groups tab, under Security Policy, on the Computer Group drop-down list, select the computer group for which you want to enable content filtering.

3 Under Content Filtering, check **Enable Content Filtering**.

4 Do one of the following:

- To filter content based on the deny list, click **Use Deny List**.
- To filter content based on the allow list, click **Use Allow List**.

5 Click **Save**.

Enabling content filtering for WAN

You enable content filtering for the WAN through VPN client tunnels.

See "Defining client VPN tunnels" on page 99.

Monitoring content filtering

Content filtering logs a message in the log files if packets are dropped due to a user attempting to access a URL on the deny list, or attempting to access a URL that is not specifically permitted on the allow list. See "Logging, monitoring and updates" on page 119.

You can view the URLs and their status that are on either the allow or deny list.

To view a list of URLs on the allow or deny list

See "Content filtering field descriptions" on page 210.

1. In the left pane, click **Content Filtering**.
2. Under Select List, under List Type, do one of the following:
   - To view the URLs on the Deny list, click **Deny**.
   - To view the URLs on the Allow list, click **Allow**.
3. Click **View/Edit**.

Chapter 8

Preventing attacks

This chapter includes the following topics:

- How intrusion detection and prevention works
- Setting protection preferences
- Enabling advanced protection settings

The Symantec Gateway Security 300 series appliance provides intrusion detection and prevention services (IDS and IPS). The IDS and IPS functions are enabled by default, and provide atomic packet protection. You may disable IDS and IPS functionality at any time.

Note: An atomic IDS and IPS signature is defined as a signature based on a single IP packet.

How intrusion detection and prevention works

The appliance defends against and logs fragmentation attacks, IP option attacks, buffer overflow attacks, port scans, oversize packet spoof, and flood attacks.

Any traffic arriving on the inside or outside the unit with an uncommon set of IP options settings is blocked.

IDS/IPS logs events which are identified in the Status screen. WAN-side IDS/IPS logging is enabled by default. If IDS logging is disabled, the appliance still blocks any connection attempt to an unauthorized service for inbound connections. However, when the Trojan horse lookup service is disabled, and only an access denied message is logged.

The number of log messages that are tracked depends on the attack type. Unlimited management login attempts are logged. Attack logging is limited to

one attack in five seconds. When ICMP is enabled, the log messages are not limited.

The appliance defends against the following atomic IDS/IPS signatures:

- Bonk
- Back Orifice (Trojan horse communication channel)
- Girlfriend (Trojan horse communication channel)
- Fawx
- Jolt
- Land
- Nestea
- Newtear
- Overdrop
- Ping of Death
- Portal of Doom (Trojan horse communication channel)
- SubSeven (Trojan horse communication channel)
- Syndrop
- Teardrop
- Winnuke
- HTML buffer overflow
- TCP/UDP flood protection

Trojan horse protection

Any attempt to connect to a blocked port that is commonly used by Trojan horse programs is logged and classified as a possible attack. The log message warns the user that an illegal connection attempt was made and that they should audit their internal systems to verify they are not compromised. Trojan horse protection is overridden if traffic is explicitly allowed in an inbound rule.

Setting protection preferences

For each atomic IDS/IPS signature, you can set the action to take with detection of each individual signature, as follows:

- Block and Warn
  Drop and log packets identified as containing the specific signature.

- Block/Don't Warn
  Drop the packet; but do not log.

You can configure the following options for enabling and disabling IDS/IPS signature detection and logging:

- Select All to enable or disable detection of ALL signatures.
- Enable/disable detection of each signature individually.

To set protection preferences

See "IDS Protection tab field descriptions" on page 205.

1. In the SGMI, in the left pane, click **IDS/IPS**.
2. In the right pane, on the IDS Protection tab, under IDS Signatures, from the Name drop-down list, select an IDS signature.
   To apply the preferences to all the signatures, click **>>Select All<<**.
3. Under Protection settings, next to Action, select an action.
4. Next to Protection Area, select an interface to protect.
5. Click **Update**.

Enabling advanced protection settings

Advanced protection settings help you protect your network beyond attacks that can be identified by atomic signatures.

IP spoofing protection

Any non-broadcast or multicast packet arriving on a WAN interface with a source IP address that matches any internal subnet is blocked and flagged as an IP spoofing attempt. Internal subnets are derived from the LAN side subnet address of the appliance and the static route entries on the appliance for the LAN interface.

Likewise, any non-broadcast or non-multicast traffic that arrives at the internal or wireless interface with a source IP address that does not match any predefined internal network is blocked and logged as an internal IP spoofing attempt. Internal networks are derived from static routes on the unit and the internal LAN/WLAN address of the unit. Spoof protection can be disabled for the internal LANs and WAN.

To configure IP spoof protection

See "IDS Protection tab field descriptions" on page 205.

1. In the SGMI, in the left pane, click **IDS/IPS**.
2. In the right pane, on the Advanced tab, under IP Spoof Protection, check **WAN** or **WLAN/LAN**.
3. Click **Save**.

TCP flag validation

Certain port mapping tools, such as NMAP, use invalid TCP flag combinations to detect a firewall on a network or map the security policy implemented on the firewall. Symantec Gateway Security 300 Series blocks and logs any traffic with illegal flag combinations for traffic that is not being denied by the security policy. Any traffic denied by the security policy that has one or more bad TCP flag combinations is classified as one of several NMAP port scanning techniques (NMAP Null Scan, NMAP Christmas Scan, and so on).

To enable TCP flag validation

See "IDS Protection tab field descriptions" on page 205.

1. In the SGMI, in the left pane, click **IDS/IPS**.
2. In the right pane, on the Advanced tab, under TCP Flag Validation, check **Enable**.

Chapter 9

Logging, monitoring and updates

This chapter includes the following topics:

- Managing logging
- Updating firmware
- Backing up and restoring configurations
- Interpreting LEDs
- LiveUpdate and firmware upgrade LED sequences

The appliance provides configurable system logging features for viewing the system logs and monitoring system status.

Managing logging

The firewall, IDS, IPS, VPN, content filtering, and AVpe features of the product log messages when certain events occur. You can configure which events are logged so that you view only the log messages that you need.

You can view these log messages through the SGMI, or forward them to external services. Log messages are maintained until the appliance is restarted. On all appliances, the 100 most current messages are available to view. On models 360 and 360R, the most current 100 log events are maintained, even if the appliance is restarted.

When the log is full, new entries overwrite the oldest ones. You should set up either email forwarding or a Syslog server if you want to retain old log messages. See "Emailing log messages" on page 120 or "Using Syslog" on page 121.

Configuring log preferences

Logging preferences let you set the way that you view log messages, the amount of logging that is performed, and how to handle when the log becomes full. The following settings help you create logging scenarios that are appropriate to your network's needs:

- Emailing log messages
- Using Syslog
- Configuring and verifying SNMP
- Selecting logging levels
- Setting log times

Emailing log messages

You can configure the appliance to automatically email log entries when the log is full or if an attack is detected. The log file is sent as a text message.

To configure email forwarding

See "Log Settings tab field descriptions" on page 155.

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. On the right pane, on the Log Settings tab, in the SMTP Server text box, type the IP address or DNS name of the SMTP server you want to receive the Log file.
3. In the Send Email From text box, type the email address of the sender of the email.
4. In the Send Email To text box, type the email address of the receiver of the email.
5. Click **Save**.
6. To send the current log messages without waiting for the log to become full, click **Email Log Now**.

Using Syslog

Sending log messages to a Syslog server lets you store log messages for long term. A Syslog server listens for log entries forwarded by the appliance and stores all log information for future analysis. The Syslog server can be on the LAN or WAN, or behind a VPN tunnel.

Note: The date and time on messages in the Syslog server are the time they arrived at the Syslog server, and not the time that the appliance logged the event that triggered the log message.

To use Syslog

See "Log Settings tab field descriptions" on page 155.

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Log Settings tab, under Syslog, in the Syslog Server text box, type the IP address of a host running a standard Syslog utility to receive the log file.
3. Click **Save**.

Configuring and verifying SNMP

The appliance supports Simple Network Management Protocol (SNMP) version 1.0 and generates network event alert messages, copies them into an SNMP TRAP or GET with the associated community name, and then sends them to registered SNMP servers. This capability lets the appliance report status information to network-wide SNMP-based management applications. The appliance generates SNMP messages for the following events:

- Cold start-up of the appliance
- SGMI authentication failure
- Ethernet WAN ports up and down
  - No trap when WAN ports comes alive as part of system startup
  - WAN disconnect
  - WAN coming back after a previous disconnect
- Serial WAN port (PPPoE or Analog)
  - WAN Link up (connected)
  - WAN Link down (disconnected)

A GET is a request from the SNMP server for status information from the Symantec Gateway Security 300 Series appliance. The appliance supports all

SNMP v1 MIBS (information variables) using GETs. A TRAP collects status information set from Symantec Gateway Security 300 Series appliance to the SNMP server.

Configuring SNMP sets the IP addresses of the SNMP servers to receive status information (TRAPS) alerts from the SNMP agent running on the appliance. This feature provides minimal protection over a public network. Therefore for highest security, remote access administration should be done through a VPN tunnel.

To monitor the appliance on the LAN side, browse to the appliance's LAN IP address (by default, 192.168.0.1) using an SNMP v1 MIB browser. To allow external access to SNMP GET on the appliance, check Enable Remote Monitoring.

To configure SNMP

There are two parts to configuring SNMP:

- Configuring SNMP
- Verifying communication between the SNMP server and the Symantec Gateway Security 300 Series appliance.

Before you begin configuring SNMP, collect the following information:

- For TRAPs, you must have SNMP v 1.0 servers or applications running on your network to receive the network event alert messages and you need the SNMP server IP addresses to configure SNMP on the appliance.
- You also need the community string for the SNMP server. The SNMP server IP address and community string should be available from the administrator running the SNMP server.
- You can configure SNMP at anytime after the appliance is installed and the SNMP servers are running.

See "Administration field descriptions" on page 157.

To configure SNMP

1. In the left pane, click **Administration**.
2. In the right pane, on the SNMP tab, under SNMP Read-only Managers (GETS and TRAPS), in the Community String text box, type the name of the community.
   The default is Public.
3. In the IP Address text boxes, type the IP addresses of the SNMP read-only managers (for TRAP collection only).
4. Click **Save**.

To verify SNMP communication

- Contact the SNMP server administrator and have them send a GET from the SNMP server to your appliance.

The appliance responds by sending status information to the SNMP server.

If it does not respond, check that the SNMP server IP address and community string are correct. Also check that the SNMP server is accessible from the appliance.

Selecting logging levels

The log file contains only the types of information you choose. This is useful for isolating a problem or attack.

If you select Debug information, performance may be affected by the number of messages that are created. You should select this option only for troubleshooting purposes, and then disable it when you are done.

To select log levels

See "Logging/Monitoring field descriptions" on page 151.

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Log Settings tab, under Log Type, check the types of information you want to be logged.
3. Click **Save**.

Setting log times

Network Time Protocol (NTP) is an Internet standard protocol that ensures accurate synchronization to the millisecond of computer clock times in a network.

If you do not configure an NTP server, standard public NTP servers are used. If an NTP server is not reachable, when an event occurs, the appliance records the time (in seconds) since the last reboot.

To set log times

See "Log Settings tab field descriptions" on page 155.

1. In the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Log Settings tab, under Time, in the NTP Server text box, type the IP address or fully qualified domain name of the non-public NTP Server.
3. Click **Save**.

Managing log messages

The View Log tab shows the current conditions of the appliance. Models 360 and 360R have a WAN 2 section for the second WAN port status.

The information on the View Log tab is current when you click it. Conditions may change while you are viewing the screen. Refresh updates the View Log tab to display the most current messages.

You can manually delete the contents of the log at any time.

To manage log messages

After log messages have been generated, you can view them, refresh them to see the most current messages, or clear the log if you no longer want those messages.

See "View Log tab field descriptions" on page 154.

To view log messages

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. Do one of the following:
   - On the View Log tab, view the log messages.
   - To view older log messages, click **Next Page**.

To refresh log messages

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the View Log tab, click **Refresh**.

To clear log messages

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the View Log tab, click **Clear Log**.

Updating firmware

The appliance runs using a set of instructions that are coded into its permanent memory called firmware. The firmware contains all of the features and functionality of the appliance. There are two types of firmware updates: destructive and non-destructive. Destructive firmware completely overwrites the firmware and all the configuration settings. Non-destructive firmware updates the firmware but keeps the configurations intact.

Symantec periodically releases updates to the firmware. There are three ways to update the firmware on your appliance: automatically using the Scheduler in

LiveUpdate, manually using LiveUpdate, or manually by receiving firmware from Symantec Technical Support and applying it using the symcftpw tool. By default, LiveUpdate checks for updates at the end of the Setup Wizard. You may disable this feature. See the *Symantec Gateway Security 300 Series Installation Guide*.

Warning: Performing a manual firmware upgrade with app.bin may overwrite your configuration settings. Before performing an upgrade, make note of your settings. Do not use a configuration backup file of older firmware on newer firmware. LiveUpdate firmware upgrades never overwrite your configuration.

When you apply a firmware upgrade manually or through LiveUpdate, the LEDs flash in a unique sequence that indicates the progress.

See "LiveUpdate and firmware upgrade LED sequences" on page 139.

Automatically updating firmware

LiveUpdate is a Symantec technology that enables you to automatically keep your Symantec products up-to-date with the latest revision. You can configure LiveUpdate to check for updates automatically, or you can manually run LiveUpdate at any time to check for updates.

Symantec periodically releases firmware updates to ensure the highest level of security available. Run LiveUpdate as soon as your Symantec Gateway Security 300 Series is connected to the Internet.

See "Running LiveUpdate Now" on page 131.

When LiveUpdate checks for firmware updates, if a new firmware package is found, LiveUpdate downloads and begins applying the firmware without prompting the administrator. During the download and application, the SGMI displays a message stating that an update is being applied and to wait a few minutes before attempting to log into the SGMI. Afterwards, the appliance may restart. When firmware application is complete, a message is logged.

If LiveUpdate checks for firmware updates and none are available (the current firmware is up-to-date), a message is logged.

All LiveUpdate packages posted by Symantec are tested and validated by Symantec. These packages do not intentionally overwrite your current configuration. However, they require an automatic restart of the appliance. To minimize downtime or interruption to your network connectivity, use the Preferred Time feature to schedule updates during off hours.

The LiveUpdate functionality provides a fail-safe mechanism for firmware updates if the appliance becomes non-usable (such as a power outage during the

LiveUpdate upload). If the appliance is unable to pass its self-check test with a new LiveUpdate package, it reverts to the factory firmware stored in protected memory. LiveUpdate only downloads and applies non-destructive firmware.

Scheduling automatic updates

LiveUpdate runs in automatic or manual mode. In automatic mode, the appliance checks for new updates. If you schedule automatic updates, each time the appliance is restarted, LiveUpdate checks for updates. Also, if you change the appliance from manual updates to automatic, LiveUpdate checks for updates at the next time you specify in the UTC text box.

If LiveUpdate downloads and applies a new firmware update, the appliance may restart. For this reason, you should schedule automatic updates to occur during your network's down time.

To schedule LiveUpdate for automatic updates

See "LiveUpdate tab field descriptions" on page 159.

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the LiveUpdate, under Automatic Updates, check **Enable Scheduler**.
3. From the Frequency drop-down list, select the frequency with which the appliance checks for updates.
4. In the Preferred Time (UTC) text box, type the time of day, in hours and minutes, that you want the appliance to check for updates.
5. Click **Save**.

Allowing automatic updates through an HTTP proxy server

LiveUpdate optional settings let you configure a connection to a LiveUpdate server through an HTTP proxy server. Use this feature only in the following situations:

- The appliance is located behind a Symantec Gateway Security appliance using an HTTP proxy server.
- The appliance is located behind a third party device using HTTP proxy server.
- Your ISP uses an HTTP proxy server.

For more information, refer to Symantec LiveUpdate documentation.

See "LiveUpdate tab field descriptions" on page 159.

To allow automatic updates through an HTTP proxy server

1. In the SGMI, in the left pane, click **Administration**.
2. In the right pane, on the LiveUpdate tab, under Optional Settings, check **HTTP proxy Server.**
3. In the Proxy Server Address text box, type IP address or fully qualified domain name of the HTTP proxy server.
4. In the Port text box, type the port number.
5. In the User Name text box, type the proxy user name.
6. In the Password text box, type the proxy password.
7. Click **Save**.

Changing the LiveUpdate server location

By default, the LiveUpdate settings point to liveupdate.symantec.com.You can also configure the appliance to use your own LiveUpdate staging server instead of the Symantec LiveUpdate site.

The internal LiveUpdate servers shown in Figure 9-1 are configured using the Symantec LiveUpdate Administration Utility. Rather than the appliance contacting the Symantec servers to obtain product updates, the appliance can contact the LiveUpdate server on the local network. This greatly reduces network traffic and increases transfer speeds. It also lets you stage, manage, and validate updates before applying them. The LiveUpdate Administration Utility

and instructions for installation are available on the Symantec Technical Support Web page http://www.symantec.com/techsupp/.

Figure 9-1 shows several possible LiveUpdate configurations.

Figure 9-1 LiveUpdate configurations

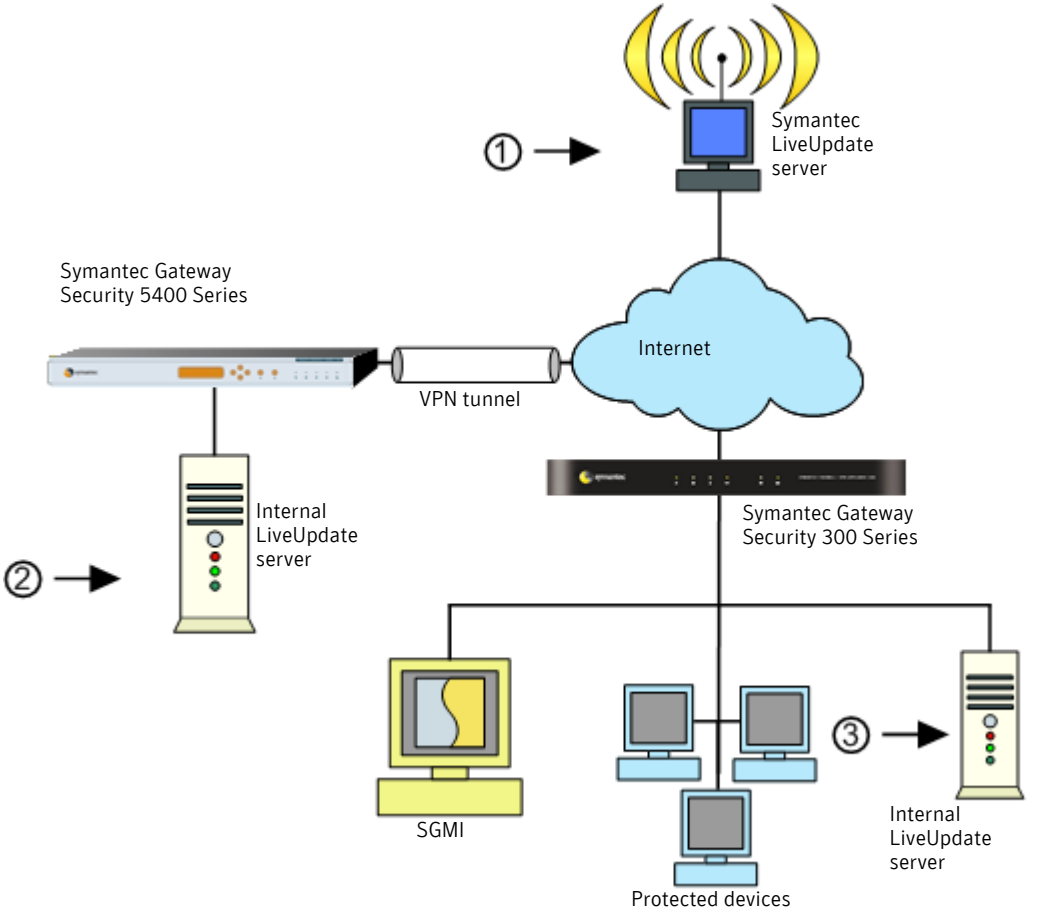


Table 9-1 shows and lists the LiveUpdate server configurations shown in Figure 9-1.

Table 9-1 LiveUpdate server configurations

Location	Description
1	Symantec LiveUpdate server: http://liveupdate.symantec.com. This is the standard Symantec corporate LiveUpdate site which broadcasts firmware availability. It is the default configuration in your appliance.
2	Internal Live Update server at a remote internal location, protected by a VPN tunnel.
3	Internal LiveUpdate server at a local location.

LiveUpdate servers can be on the WAN or LAN, or accessible through a Gateway-to-Gateway VPN tunnel.

See "LiveUpdate tab field descriptions" on page 159.

To change the LiveUpdate server location

1. In the left pane, click **Administration**.
2. In the right pane, on the LiveUpdate tab, under General Settings, in the LiveUpdate Server text box, type the IP address or fully qualified domain name for your LiveUpdate server.
3. Click **Save**.

Upgrading firmware manually

Firmware upgrades are available from Symantec's Web site. If you do not configure LiveUpdate to automatically download and apply firmware upgrades, or if you are instructed to manually perform an upgrade by Symantec Technical Support, you should check the Symantec Web for the latest version of the firmware. Your current firmware version number is available from the Status screen.

The firmware file that is available from Symantec Technical Support is called all.bin. It overwrites your configuration, so before you begin a manual firmware

upgrade, make note of your configuration. The only setting that it leaves intact is the administrator's password.

See "Setting the administration password" on page 16.

Warning: Re-flashing the firmware with an old version of the firmware erases all previous configuration information including the password.

Apply the firmware by using the Symantec FTP utility (included on the Symantec Gateway Security 300 Series CD-ROM), or you can use the DOS TFTP command with the -i (binary) option. This transfers the firmware file to the appliance, applies it, and then restarts the appliance.

Flashing the firmware

Before you perform a manual firmware upgrade, ensure you have the following items:

- symcftpw utility
  Located on the Tools folder on the CD-ROM included with your appliance. You may also use the TFTP command to put firmware on the appliance.
- Firmware file
  Download the latest firmware file from Symantec's Web site.

Note: If the computer on which you run symcftpw has Norton Internet Security installed, you must configure both an inbound rule and an outbound rule in Norton Internet Security to permit the traffic between the computer and the appliance.

Figure 9-4 shows the rear panel on model 320. This graphic is for reference; the full description of each feature is available in the *Symantec Gateway Security 300 Series Installation Guide*.

Figure 9-2 Model 320 rear panel

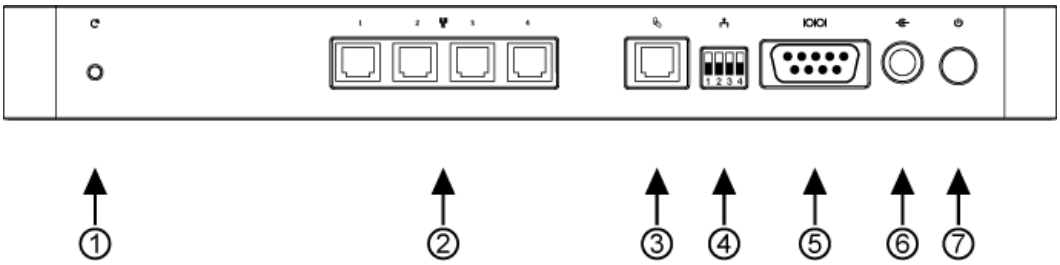
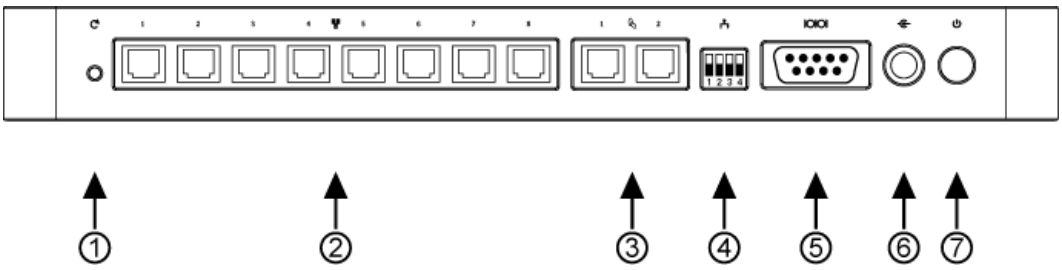


Figure 9-5 shows the rear panel of models 360 and 360R. This graphic is for reference; the full description ofeach feature is available in the *Symantec Gateway Security 300 Series Installation Guide.*

Figure 9-3 Model 360 and 360R rear panel



To flash the firmware

1. To turn off the power, press the power button on the back panel of the appliance.
2. Turn DIP switches 1 and 2 (4) to the on (up) position.
3. To turn on the power, press the power button (7).
4. Copy the firmware file and the symcftpw utility into a temporary folder on your hard drive.
5. Double-click the symcftpw icon.
6. In the Server IP text box, type the IP address of the appliance.
   The default IP address of the appliance is 192.168.0.1.
7. In the Local File text box, type a file name for the firmware upgrade file.
8. Click **Put**.
   Wait several minutes before restarting the appliance. Flashing is complete when symcftpw reports that flashing is complete, LEDs 2 and 3 stop flashing alternately, the appliance has restarted, and then LEDs 1 and 3 are illuminated steadily. This may take several minutes.
9. Turn DIP switches 1 and 2 (4) to the off position (down).

Running LiveUpdate Now

Run LiveUpdate Now is the manual LiveUpdate feature. Run LiveUpdate Now immediately checks for the latest firmware updates for your appliance and installs it. If you are already running the latest version, it does not update your appliance. LiveUpdate updates retain your configuration.

You can also change the address of the LiveUpdate server to check.
See "Changing the LiveUpdate server location" on page 127.

To run LiveUpdate now

See "LiveUpdate tab field descriptions" on page 159.

1. In the left pane, click **Administration**.
2. In the right pane, on the LiveUpdate tab, under Status, click **Run LiveUpdate Now.**

Forcing a firmware update

If manually flashing the firmware does not work, you can force the firmware on to the appliance. Do this only if flashing firmware as instructed in "Flashing the firmware" on page 130 does not work, or if you are instructed to do so by Symantec Technical Support.

Use Figure 9-6 and Figure 9-7 for reference in the following procedure.

To force a firmware update

1. Note all of your configuration settings.
2. To turn off the power, press the power button on the back panel of the appliance.
3. Turn DIP switches 2 and 4 (4) to the on (up) position.
4. To turn on the power, press the power button (7).
5. On the LAN computer from which you will TFTP the firmware to the appliance, change its IP address to a static IP address outside the default IP address range (192.168.0.2-1.92.168.0.52).
   Also, do not give the computer the static IP address 192.168.0.1.
6. Copy the firmware file and the symcftpw utility into a temporary folder on your hard drive.
7. Double-click the symcftpw icon.
8. In the Server IP text box, type the IP address of the appliance.
   The default IP address of the appliance is 192.168.0.1.
9. In the Local File text box, type a file name for the firmware upgrade file.
10. Click **Put**.
    Wait several minutes before restarting the appliance. Flashing is complete when symcftpw reports that flashing is complete, LEDs 2 and 3 stop flashing alternately, the appliance has restarted, and then LEDs 1 and 3 are illuminated steadily. This may take several minutes.

11 Turn DIP switches 2 and 4 (4) to the off position (down).

Checking firmware update status

The Status section shows the date and version of the last firmware update. The last update shows the date and time (if an NTP service is available) of the last LiveUpdate check. This check may or may not have resulted in a new firmware version being downloaded depending on whether the appliances firmware is already the most recent version.

For automatic updates, LiveUpdate logs messages for the following events:

- Successfully downloading the firmware package
- Unsuccessfully downloading the firmware package
- No new firmware package available; every component is current

If a LiveUpdate fails because of an HTTP error, the failure is logged along with the HTTP error message reported by the HTTP client.

To check firmware update status

Knowing the version of the firmware on the appliance is important if you plan to contact Symantec Technical Support.

See "LiveUpdate tab field descriptions" on page 159.

See "Status tab field descriptions" on page 152.

To view LiveUpdate firmware package status

1 In the left pane, click **Administration**.

2 In the right pane, on the LiveUpdate tab, under Status, view the date of the last update and the version number.

To view the current version of the firmware on the appliance

1 In the left pane, click **Logging/Monitoring**.

2 In the right pane, on the Status tab, under Unit, view the Firmware Version.

Backing up and restoring configurations

You can back up your appliance configuration at any time. You should do this after you initially configure the appliance or before changing the configuration significantly.

Note: You should not use a configuration backup file from an older version of the firmware to restore your settings unless instructed to do so by Symantec Technical Support.

The backup file is created in the same folder on your hard drive where you put the symcftpw application. In the symcftpw application, you can specify where to store the backup file, such as a a floppy disk. This is useful to store the configuration in a safe location, such as a fire-safe box.

To back up and restore configurations

Backing up your configuration is good practice to ensure that you can restore the configuration if the appliance fails.

To back up an appliance configuration

1. To turn off the power, press the power button on the back panel of the appliance.
2. Turn DIP switches 1 and 2 to the on (up) position.
3. Turn on the appliance by pressing the power button.
4. Copy the symcftpw utility from the CD-ROM to a folder on your hard drive.
5. Double-click the symcftpw icon.
6. In the Server IP text box, type the IP address of the appliance.
   The default IP address of the appliance is 192.168.0.1.
7. In the Local File text box, type a file name for the backup file.
8. Click **Get**.
9. Turn DIP switches 1 and 2 to the off (down) position.
10. Copy the backup file from your hard drive to a floppy disk and store in a secure location.

To restore an appliance configuration

1. To turn off the power, press the power button on the back panel of the appliance.
2. Turn DIP switches 1 and 2 to the on (up) position.
3. Turn on the appliance by pressing the power button.
4. Copy the symcftpw utility from the CD to a folder on your hard drive.
5. Double-click the symcftpw icon.
6. In the Server IP text box, type the IP address of the appliance.

The default IP address of the appliance is 192.168.0.1.

7 In the Local File text box, type a file name for the backup file.

8 Click **Get**.

9 Turn DIP switches 1 and 2 to the off (down) position.

Resetting the appliance

You can reset the appliance in three different ways:

- Basic reset
  Restarts the appliance. This is similar to turning off and then turning on the appliance. All current connections, including client VPN tunnels, are lost. Previously connected Gateway-to-Gateway VPN tunnels are reestablished when the appliance restarts. Also, the appliance performs a self-test of the hardware when the appliance restarts.
- Reset to the default configuration
  The LAN subnet IP address is reset to 191.168.0.0, the LAN IP address of the appliance is reset to 192.168.0.1, the DHCP server functionality is enabled, and the administrator's password is reset to blank.
- Reset to the reserved application
  The firmware resets to the last all.bin firmware file that was used to flash the appliance. This is either the factory firmware or a firmware upgrade that you downloaded from the Symantec Web site and applied to the appliance.

  Note: LiveUpdate does not download and apply all.bin firmware upgrades.

To reset the appliance

There are three types of factory reset, which you can perform using a combination of the DIP switches and the reset button. You must use a paper clip or pen tip to press the reset button. Refer to Figure 9-4 and Figure 9-5 for the location of the reset button and DIP switches.

Figure 9-4 shows the rear panel on model 320. This graphic is for reference; the full description of each feature is available in the *Symantec Gateway Security 300 Series Installation Guide*.

Figure 9-4 Model 320 rear panel

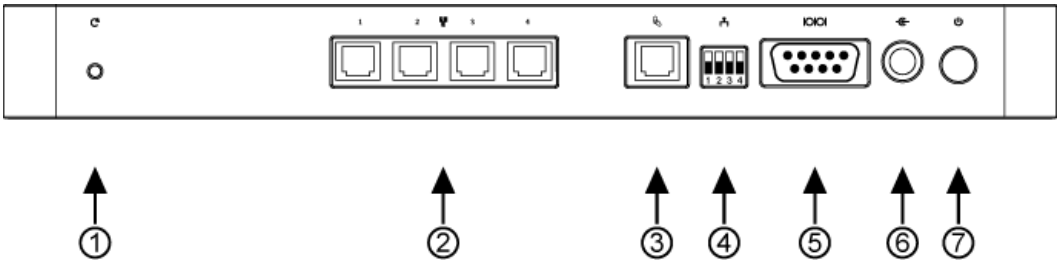
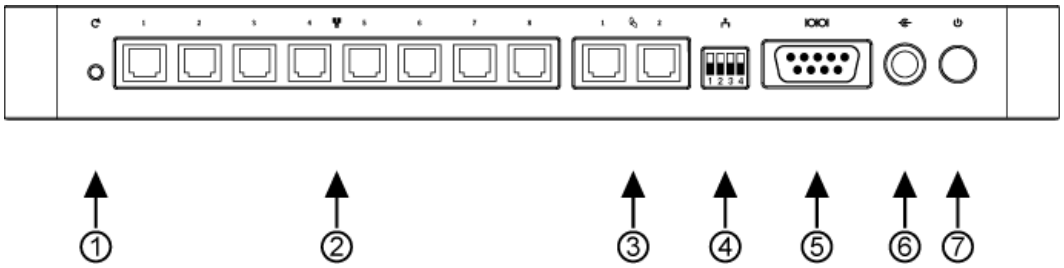


Figure 9-5 shows the rear panel of models 360 and 360R. This graphic is for reference; the full description ofeach feature is available in the *Symantec Gateway Security 300 Series Installation Guide*.

Figure 9-5 Model 360 and 360R rear panel



To perform a basic reset

- On the rear panel of the appliance, quickly press the reset button (1).

To perform a reset to the default configuration

- On the rear panel of the appliance, press the reset button (1) and hold it for five seconds.

To perform a reset to the reserved application

1. On the rear panel of the appliance, turn DIP switch 4 (4) to on (up).
2. Quickly press the reset button (1).

Interpreting LEDs

The LEDs on the front of each appliance indicate the status of the appliance. There are six LEDs; four for the appliance, and two for wireless. The wireless

LEDs generally only illuminate when the a compatible Symantec Gateway Security WLAN Access Point option is inserted.

Figure 9-4 shows the rear panel on model 320. This graphic is for reference; the full description of each feature is available in the *Symantec Gateway Security 300 Series Installation Guide*.

Figure 9-6 Model 320 rear panel

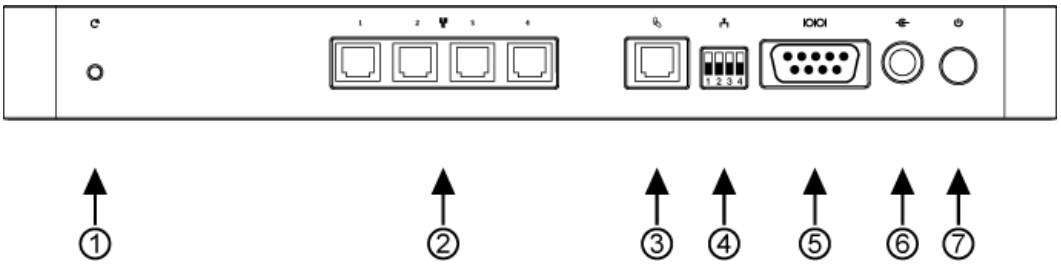


Figure 9-5 shows the rear panel of models 360 and 360R. This graphic is for reference; the full description ofeach feature is available in the *Symantec Gateway Security 300 Series Installation Guide*.

Figure 9-7 Model 360 and 360R rear panel

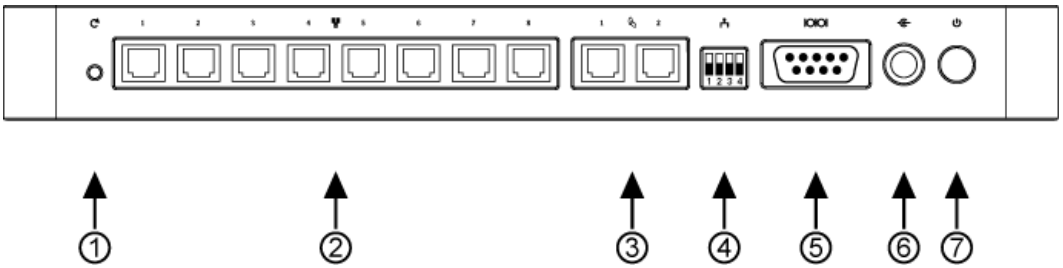


Table 9-2 describes each LED.

Table 9-2 LEDs

Location	Symbol	Feature	Description
1	⚡	Power	Illuminates when the appliance is turned on.

Table 9-2 LEDs

Location	Symbol	Feature	Description
2		Error	Illuminates if there is a problem with the appliance.
3		Transmit	Illuminates or flashes when traffic is being passed over the LAN or WAN ports.
4		Backup	Illuminates or flashes when the serial port is being used or is not functioning correctly.
5		Wireless-ready	Illuminates when the wireless card is inserted and functioning properly.
6		Wireless-active	Illuminates or flashes when the wireless card is transmitting or receiving data.

The LEDs on the front panel of the appliance have three states: solid on, flashing, and solid off. The combination of the Error and Transmit LED states indicate the status of the appliance. Table 9-3 describes the LEDs state combinations and appliance status that they indicate.

Table 9-3 LEDs states and appliance status

Error LED (2) state	Transmit LED (3) state	Appliance status
Solid off	Solid on	Normal operation.
Solid off	Flashing	Transmitting/receiving Data from LAN.
Flashing	Flashing	■ MAC address not assigned. ■ Firmware problem. Appliance is ready for a forced download. ■ Appliance detected an error and cannot recover.
Flashing	Solid on	Configuration mode.

Table 9-3 LEDs states and appliance status

Error LED (2) state	Transmit LED (3) state	Appliance status
Solid on	Solid on	Hardware problem.
Flashing once	Solid off	RAM error.
Flashing twice	Solid off	Timer error.
Flash three	Solid off	DMA error.
Solid on	Flashing once	LAN error.
Solid on	Flashing twice	WAN error.
Solid on	Flashing three	Serial error.
Solid off	Solid off	No power.
Both flashing alternatively		■ Download in progress. ■ Appliance is writing to flash.

LiveUpdate and firmware upgrade LED sequences

When you apply a firmware upgrade using the symcftpw utility or TFTP, or if LiveUpdate is downloading and applying a firmware upgrade, there is a unique sequence of LED flashing that indicates the progress.Table 9-4 describes the sequences.

Table 9-4 LiveUpdate LED sequences

Description	Power	Error	Transmit
Firmware retrieval from the Internet using LiveUpdate or uploading it using the symcftpw or TFTP tools.	On	On	Flashing when there is traffic.
Firmware downloaded and verified. This takes approximately 10 seconds.	On	Off	Off
Applying the firmware. The amount of time this takes depends on the model.	On	Flashing alternately with Transmit	Flashing alternately with Error
Update complete.	On	On	On
Appliance resets. All LEDs illuminate, and then go to the normal operation pattern.	On	Off	Flashing when there is traffic.

Appendix A

Troubleshooting

This chapter includes the following topics:

- About troubleshooting
- Accessing troubleshooting information

About troubleshooting

The Debug information feature provides a high level of detail of the system events information in the log. Debug mode gives more detailed information in the status log that is useful for Symantec Technical Support or for troubleshooting. The default user mode provides general information about actions taken defined by the security policy.

Warning: Enabling debug mode increases the number of log events and impacts performance. By design, all debug messages are in English only. Only use debug mode temporarily for troubleshooting purposes, and disable it immediately after debugging.

The Forward WAN packets to LAN feature broadcasts all WAN side packets into the LAN for packet capturing (sniffing). This is a potential security issue, so ensure that you disable this feature when you are done troubleshooting.

The security gateway also provides both PING and DNS Lookup testing tools to verify network connectivity and DNS resolution.

Note: The PING troubleshooting tool should only be used to issue PING commands to other IP addresses; you cannot PING the appliance itself.

The Result section of the Troubleshooting window shows the result of running a PING or DNS Lookup test.

To troubleshoot Symantec Gateway Security 300 Series appliances

- See "Logging/Monitoring field descriptions" on page 151.
- See "Troubleshooting tab field descriptions" on page 156.

To set logging levels

1. In the SGMI, in the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Log Settings tab, under Log Type, check the information to log.
   Debug information captures a great deal of information. Use this option only during troubleshooting.
3. Click **Save**.

To enable forward WAN packets to LAN

1. In the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Troubleshooting tab, under Broadcast Debug Level, check **Forward WAN packets to LAN**.
   Forwarding packets received on the WAN ports to the LAN for troubleshooting purposes may allow traffic normally denied by the security gateway into your internal network. You should only use this method for capturing WAN packets if you are unable to use a sniffer in the WAN side of your network. Only enable this feature as a last resort, and turn it off immediately once you complete troubleshooting.
3. Click **Save**.

To run a test

1. In the left pane, click **Logging/Monitoring**.
2. In the right pane, on the Troubleshooting tab, under Testing Tools, in the **Target Host** text box, type the IP address or DNS name you want to test.
3. In the Tool drop-down list select **PING** or **DNS Lookup**.
4. Click **Run Tool**.

The results of the test display under Result.

To test default gateway connectivity

1. Verify that your default gateway is reachable by issuing a PING request to its IP address.
2. If you can not PING a host by its IP address you either have an ISP link problem or a routing problem.

3 If you can PING a host by IP address but not by DNS name, you have a DNS server misconfiguration or the DNS server is not reachable (try to PING the DNS server by IP address to verify connectivity).

4 If you can successfully resolve some DNS names but not others, the most likely problem is not your configuration. In this case you will have to work with the authoritative Source for that DNS domain to resolve the problem.

To test WAN connectivity

1 PING the default gateway.

2 PING an Internet site by its IP address.

3 PING an Internet site by its DNS address.

Note: Some sites block PINGs on their firewalls. Make sure the site is reachable before calling your ISP or Symantec Technical Support.

Accessing troubleshooting information

Use the following procedure to access troubleshooting information from the Symantec Knowledge Base.

To access troubleshooting information

1 Go to www.symantec.com.

2 On the top of the home page, click **support.**

3 Under Product Support > enterprise, click **Continue.**

4 On the Support enterprise page, under Technical Support, click **knowledge base**.

5 Under select a knowledge base, scroll down and click **Symantec Gateway Security 300 Series**.

6 Click your specific product name and model.

7 On the knowledge base page for your appliance model, do any of the following:

- On the Hot Topics tab, click any of the items in the list to view a detailed list of knowledge base articles on that topic.
- On the Search tab, in the text box, type a string containing your question. Use the drop-down list to determine how the search is performed and click **Search**.

- On the Browse tab, expand a heading to see knowledge base articles related to that topic.

Appendix B

Licensing

This chapter includes the following topics:

- Session licensing for Symantec Gateway Security 300 Series Client-to-Gateway VPN functions
- SYMANTEC GATEWAY SECURITY APPLIANCE LICENSE AND WARRANTY AGREEMENT

Session licensing for Symantec Gateway Security 300 Series Client-to-Gateway VPN functions

Symantec Client VPN software may licensed for an appliance. The Symantec Client VPN software version must be listed as supported in the *Symantec Gateway Security 300 Series Release Notes*. The Client-to-Gateway VPN add-on is licensed by the maximum number of concurrent VPN sessions allowed. The appliance comes with a license for one Client-to-Gateway VPN session. You can purchase additional licenses for concurrent VPN sessions. For example, you may have 15 users who need VPN access as part of their normal work habits, but at any time, only 10 users are ever connected by way of the VPN.

In this situation, you only need a license for 10 concurrent VPN sessions. You must obtain additional licenses as necessary to allow the maximum number of concurrent sessions you require.You are licensed to load the client software on as many nodes as you like, but these clients are licensed for use only with the accompanying Symantec Gateway Security appliance.

Additive session licenses

Additive session licenses are available for Client-to-Gateway VPN functions. Client-to-Gateway VPN session licenses are independent of base function licenses and the maximum number of concurrent sessions may be limited by hardware performance, your network implementation or traffic characteristics.

SYMANTEC GATEWAY SECURITY APPLIANCE LICENSE AND WARRANTY AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE INCLUDED WITH THE APPLIANCE YOU HAVE PURCHASED TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") AND TO PROVIDE WARRANTIES ON THE APPLIANCE ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AND WARRANTY AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AND WARRANTY AGREEMENT CAREFULLY BEFORE USING THE APPLIANCE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, REQUESTING A LICENSE KEY OR USING THE SOFTWARE AND THE APPLIANCE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON IF APPLICABLE AND DO NOT USE THE SOFTWARE AND THE APPLIANCE.

1. Software License:

The software (the "Software") which accompanies the appliance You have purchased (the "Appliance") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You . Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Appliance and/or the Software, Your rights and obligations with respect to the use of this Software are as follows:

You may:

A. _____ use the Software solely as part of the Appliance.
B. _____ make copies of the printed documentation which accompanies the Appliance as necessary to support Your authorized use of the Appliance; and
C. _____ after written notice to Symantec and in connection with a transfer of the Appliance, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software, Symantec consents to the transfer and the transferee agrees in writing to the terms and conditions of this agreement.

You may not:

A. _____ sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
B. _____ use, if You received the Software distributed on an Appliance containing multiple Symantec products, any Symantec software on the Appliance for which You have not received a permission in a License Module; or
C. _____ use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (e.g., antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for each Software functionality which You have purchased and activated for use with the Appliance for any period for which You have (i) purchased a subscription for Content Updates for such Software functionality; (ii) entered into a support agreement that includes Content Updates for such Software functionality; or (iii) otherwise separately acquired the right to obtain Content Updates for such Software functionality. This license does not otherwise permit You to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the Software will perform on the Appliance in substantial compliance with the written documentation accompanying the Appliance for a period of thirty (30) days from the date of original purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Software returned to Symantec within the warranty period or refund the money You paid for the Appliance.

Symantec warrants that the hardware component of the Appliance (the "Hardware") shall be free from defects in material and workmanship under normal use and service and substantially conform to the written documentation accompanying the Appliance for a period of three hundred sixty-five (365) days from the date of original(purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Hardware returned to Symantec within the warranty period or refund the money You paid for the Appliance.

The warranties contained in this agreement will not apply to any Software or Hardware which:

A._____ has been altered, supplemented, upgraded or modified in any way; or
B._____ has been repaired except by Symantec or its designee.

Additionally, the warranties contained in this agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling; (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; (vii) Your failure to implement, or to allow Symantec or its designee to implement, any corrections or modifications to the Appliance made available to You by Symantec; or (viii) such other events outside Symantec's reasonable control.

Upon discovery of any failure of the Hardware, or component thereof, to conform to the applicable warranty during the applicable warranty period, You are required to contact us within ten (10) days after such failure and seek a return material authorization ("RMA") number. Symantec will promptly issue the requested RMA as long as we determine that You meet the conditions for warranty service. The allegedly defective Appliance, or component thereof, shall be returned to Symantec, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the

exterior of the shipment packaging and with the Appliance. Symantec will have no obligation to accept any Appliance which is returned without an RMA number.

Upon completion of repair or if Symantec decides, in accordance with the warranty, to replace a defective Appliance, Symantec will return such repaired or replacement Appliance to You, freight and insurance prepaid. In the event that Symantec, in its sole discretion, determines that it is unable to replace or repair the Hardware, Symantec will refund to You the F.O.B. price paid by You for the defective Appliance. Defective Appliances returned to Symantec will become the property of Symantec.

Symantec does not warrant that the Appliance will meet Your requirements or that operation of the Appliance will be uninterrupted or that the Appliance will be error-free.

In order to exercise any of the warranty rights contained in this Agreement, You must have available an original sales receipt or bill of sale demonstrating proof of purchase with Your warranty claim.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE APPLIANCE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software or the Appliance.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Appliance and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software and shall return the Appliance to Symantec. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

Appendix C

Field descriptions

This chapter includes the following topics:

- Logging/Monitoring field descriptions
- Administration field descriptions
- LAN field descriptions
- WAN/ISP field descriptions
- Firewall field descriptions
- VPN field descriptions
- IDS/IPS field descriptions
- AVpe field descriptions
- Content filtering field descriptions

Logging/Monitoring field descriptions

The Symantec Gateway Security 300 Series provides configurable system logging features and tabs for viewing the system logs and monitoring system status. It also has built-in testing tools for troubleshooting and connectivity verification.

This section contains the following topics:

- Status tab field descriptions
- View Log tab field descriptions
- Log Settings tab field descriptions
- Troubleshooting tab field descriptions

Status tab field descriptions

The Status tab shows the current conditions and settings of the security gateway.

Table C-1 Status tab field descriptions

Section	Field	Description
Model 320: WAN (External Port) Model 360/360R: WAN 1 (External Port) WAN 2 (External Port)	Connection Status	Displays whether the WAN port is connected or disconnected to the Internet or an internal network.
	Netmask	Derived from DHCP or static IP configuration.
	IP Address	Displays the IP address of the WAN port based on your local configuration.
	Physical Address	Media Access Control (MAC) address of the security gateway.
	Default Gateway	Displays an IP address based on your local configuration. Used by the security gateway to route any packets destined to any networks it does not recognize. In most configurations, this is the IP address of your ISP's router.
	DHCP Client	Displays enabled or disabled. If enabled, the security gateway uses DHCP to request an IP address, DNS server, and routing information from your ISP or intranet when you start the security gateway.
	DNS IP Address(es)	Displays an IP address provided by your ISP.
	DHCP Lease Time	If DHCP Client is enabled, this displays the amount of time the security gateway will own the IP address. This is obtained when you start the security gateway.

Table C-1 Status tab field descriptions (Continued)

Section	Field	Description
LAN (External Port)	IP Address	Displays the IP address of the security gateway. The default value is 192.168.0.1.
	Physical Address	Displays the physical address (MAC) of the security gateway's LAN's port. The default value is the factory setting.
	Netmask	Displays the network mask address as set on the LAN tab. The default value is 255.255.255.0.
	DHCP Server	Displays enabled or disabled, depending on whether the security gateway acts as a DHCP server for connected clients.
Unit	Firmware Version	Displays the factory firmware version or the firmware version from the most recent LiveUpdate or manual update.
	Language Version	Displays the factory version or the most recent update.
	Model	Displays the model number of the security gateway.
	Exposed Host	Displays enabled if you have enabled a computer on your network as an exposed host.
	Special Applications	Displays enabled or disabled. If you have configured any special applications, this field displays enabled.
	NAT Mode	Displays enabled or disabled. If you disable NAT mode, this disables the firewall security functions and the security gateway behaves as a standard router. Only use this setting for intranet security gateway deployments where, for example, the security gateway will be used as a wireless bridge on a protected network. When NAT mode is enabled, the security gateway behaves as a 802.1D network bridge device.

View Log tab field descriptions

The View Log tab shows a list of system events.

Table C-2 View Log field descriptions

Section	Field	Description
View Log	UTC Time	Coordinated Universal Time (UTC), which is the Greenwich Mean time that the message was logged. If the security gateway cannot obtain the current time from a network time protocol (NTP) server, it displays the number of seconds from when the security gateway was restarted for each event.
	Message	Displays the text of the logged event.
	Source	Displays the origin of the packet.
	Destination	Displays the intended destination of the packet.
	Note	Displays the protocol name or number or additional troubleshooting information.

Log Settings tab field descriptions

The Log Settings tab lets you configure settings that control email notification, the types of messages that are logged, and the time listed for each log message.

Table C-3 Log Settings field descriptions

Section	Field	Description
Email Forwarding	SMTP Server	IP address or fully qualified domain name of the SMTP server to use to send the log. To email logs, this is a required field.
	Send Email From	Sender's email address. The maximum number of characters is 39. To email logs, this is a required field.
	Send Email To	Receiver's email address. The maximum number of characters is 39. Include multiple receivers by separating each address with a comma. To email logs, this is a required field.
	Email Log Now	After you have typed the SMTP server, and the sender and receiver email addresses, you can click Email Log Now to send an email of the log as it is right now.
Syslog	Syslog Server	IP address of a host running a standard Syslog utility that can receive the log file.

Table C-3 Log Settings field descriptions (Continued)

Section	Field	Description
Log Type	System activity, connection status	Logs all system activity and connection status. This type is checked by default.
	Connections ALLOWED by outbound rules	Logs all connections allowed by outbound rule policies.
	Connections DENIED by outbound rules	Logs all attempted connections denied by an outbound rule policy, antivirus policy enforcement (AVpe), and content filtering.
	Connections ALLOWED by inbound rules	Logs all connections allowed by inbound rules.
	Connections DENIED by inbound rules	Logs all attempted connections denied by inbound rules.
	Detected attack	Logs all detected attacks, including port scanning, fragmentation, and Trojan horse attacks. This type is checked by default.
	Debug information	Displays additional debug information that is useful for troubleshooting. Only use this option when you are troubleshooting a problem, and then disable it after you have solved the problem.
Time	NTP Server	IP address of the non-public NTP Server.

Troubleshooting tab field descriptions

The Troubleshooting tab helps you troubleshoot your security gateway with debug options, and testing tools.

Table C-4 Troubleshooting tab field descriptions

Section	Field	Description
Broadcast Debug Level	Forward WAN packets to LAN	Enables forwarding of WAN packets to LAN. This is useful to check the WAN packets for troubleshooting without having to set up additional equipment.

Table C-4 Troubleshooting tab field descriptions (Continued)

Section	Field	Description
Testing Tools	Target Host	IP address or fully qualified domain name of host you are testing with one of the tools. The address is not validated, so ensure that you type the address accurately.
	Tool (Model 320)	Troubleshooting tools. Options include: ■ PING ■ DNS Lookup Click Run Tool.
	Tool (Model 360/ 360R)	Troubleshooting tools. Options include: ■ PING ■ DNS Lookup Click Run thru WAN 1 or Run thru WAN 2, depending which WAN port you want to troubleshoot.
Result	Result	Displays result of tool test.

Administration field descriptions

The Administration feature of the security gateway lets you manage administrator access to the SGMI with a password and allowed IP addresses. You can also configure SNMP for system monitoring and LiveUpdate to receive firmware updates.

This section contains the following topics:

■ Basic Management tab field descriptions
■ SNMP tab field descriptions
■ LiveUpdate tab field descriptions

Basic Management tab field descriptions

The Basic Management tab helps you control access to the SGMI with the administration password and allowed IP addresses.

Table C-5 Basic Management tab field descriptions

Section	Field	Description
Administration Password	admin's Password	Password used to access the SGMI. The user name is always admin. The login is case-sensitive.
	Verify Password	Retype the admin's password.
Remote Management	Start IP Address	First IP address in the range of addresses that you permit to access the SGMI. To delete an IP address, enter 0 in each of the text boxes.
	End IP Address	Last IP address in the range of addresses that you permit to access the SGMI. To delete an IP address, enter 0 in each of the text boxes.
	Allow Remote Firmware Upgrade	Allows a firmware upgrade from the range of IP addresses.

SNMP tab field descriptions

The SNMP tab lets you configure your security gateway for monitoring with SNMP servers.

Table C-6 SNMP tab field descriptions

Section	Field	Description
SNMP Read-only Managers (GETS and TRAPS)	Community String	A community string may be required by your SNMP server.
	IP Address 1, IP Address 2, IP Address 3	IP address of SNMP TRAP receivers. TRAPs are forwarded to these addresses.
	Enable Remote Monitoring	Allows external access to SNMP GET on the appliance.

LiveUpdate tab field descriptions

The LiveUpdate tab lets you configure your connection to a LiveUpdate server and schedule firmware updates for your security gateway.

Table C-7 LiveUpdate tab field descriptions

Section	Field	Description
General Settings	LiveUpdate Server	IP address or fully qualified domain name of the LiveUpdate server from which to get firmware updates. The default address is http://liveupdate.symantec.com.
Automatic Updates	Enable Scheduler	Enables the LiveUpdate scheduler. This lets you schedule times for the security gateway to automatically check for firmware updates, and then apply them.
	Frequency	Frequency with which the security gateway checks for updates. The start time for the frequency is based on the most recent reboot of the appliance. Options include: ■ Daily ■ Weekly ■ Bi-weekly ■ Monthly
	Preferred Time (UTC)	Time in hours and minutes at which the security gateway automatically checks for updates. The format is HH:MM, where HH is hours between 0 and 24, and MM is minutes between 0 and 59. For example, to check for updates at 7:30 pm, type 19:30. The UTC setting is dependent on access to an NTP server. Use only numeric characters and a colon in this text box.

Table C-7 LiveUpdate tab field descriptions (Continued)

Section	Field	Description
Optional Settings	HTTP Proxy Server	Enables the security gateway to contact the LiveUpdate server through a HTTP proxy server.
	Proxy Server Address	IP address of the HTTP proxy server through which the LiveUpdate server gets the firmware updates.
	Port	Port number associated with the HTTP proxy server through which the LiveUpdate server gets the firmware update. The maximum value is 65535. The default port is 80.
	User Name	User name associated with the HTTP proxy server through which LiveUpdate gets the firmware update.
	Password	Password associated with the HTTP server.
Status	Last Update	Date of the most recent update.
	Last Update Version	Version number of the most recent update.

LAN field descriptions

LAN settings let you configure your security gateway to work in a new or existing internal network. LAN settings include the security gateway's IP address, whether it acts as a DHCP server for the nodes it protects, and LAN port settings.

This section contains the following topics:

- LAN IP & DHCP tab field descriptions
- Port Assignment tab field descriptions

LAN IP & DHCP tab field descriptions

The LAN IP & DHCP tab lets you set the security gateway's IP address and configure the security gateway to act as a DHCP server.

Table C-8 LAN IP & DHCP tab field descriptions

Section	Field	Description
LAN IP	IP Address	IP address of the security gateway's internal interface. The current IP address appears in the text boxes. The default value is 192.168.0.1. You cannot set the security gateway's IP address to 192.168.1.0.
	Netmask	Security gateway netmask. The current netmask appears in the text boxes. The default value is 255.255.255.0.
DHCP	DHCP Server	Makes the security gateway act as a DHCP server. To use another DHCP server, or if the clients use static IP addresses, click Disable.
	Range Start IP Address	First IP address in the range of IP addresses that you want the security gateway to assign to clients. For example, if you want the security gateway to assign IP addresses in the range 172.16.0.2 to 172.16.0.75, type 172.16.0.2 in the Range Start IP Address text boxes.
	Range End IP Address	Last IP address in the range of IP addresses that you want the security gateway to assign to clients. In the previous example, type 172.16.0.75 in the Range End IP Address text boxes.
DHCP Table	Host Name	Name of the computer to which the security gateway assigned an IP address.
	IP Address	IP address from the indicated range that the security gateway assigned to the computer.
	Physical Address	Physical (MAC) address of the network interface card (NIC) in the computer that was assigned an IP address.
	Status	Status of the DHCP lease on the IP address that was assigned to the computer. Options are: ■ Leased ■ Reserved

Port Assignment tab field descriptions

Port assignments let you specify if the LAN port resides on a trusted or untrusted VLAN. The trusted VLAN is for wired connections and the non-trusted is for wireless connections.

Table C-9 Port Assignment tab field descriptions

Section	Field	Description
Physical LAN Ports	Port 1, Port 2, Port 3, Port 4 (Model 320) Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8 (Model 360/360R)	Assigns ports on the switch function of the security gateway as trusted or untrusted. This enables wireless and wired LAN-based VPN security through the port-based virtual network capabilities of the switch function on the security gateway, in addition to support for LAN-side global tunnels directly to the wireless interface. The tunnel endpoint will be at the main gateway for each LAN network subnet. Options include: ■ Standard Use this assignment for all non-wireless LAN devices. All traffic is implicitly trusted and allowed to pass between VLANs. ■ SGS Access Point Secured Enables VPN security to be enforced at the roaming access point or switch level. ■ Enforce VPN tunnels/Allow IPsec pass-thru Explicit untrusted association. Requires a mandatory tunnel between the wireless VPN client and the security gateway. IPsec traffic is allowed to pass through a subsidiary switch with tunnel termination points located at the primary security gateway and the client.

WAN/ISP field descriptions

The Symantec Gateway Security 300 Series WAN/ISP functionality provides connections to the outside world. This can be the Internet, a corporate network, or any other external private or public network. WAN/ISP functionality can also be configured to connect to an internal LAN when the security gateway is protecting an internal subnet.

This section contains the following topics:

- Main Setup tab field descriptions
- Static IP & DNS tab field descriptions
- PPPoE tab field descriptions
- Dial-up Backup & Analog/ISDN tab field descriptions
- PPTP tab field descriptions
- Dynamic DNS tab field descriptions
- Routing tab field descriptions
- Advanced tab field descriptions

Main Setup tab field descriptions

On the Main Setup tab, you select your connection type and configure the security gateway's identification settings.

Table C-10 Main Setup tab field descriptions

Section	Fields	Description
Model 320: Connection Type Model 360/360R: WAN1 (External) or WAN2 (External)	Connection Type	The following connection types are supported: ■ DHCP (Auto IP) Your ISP assigns you an IP address automatically each time you connect. ■ PPPoE Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on an Ethernet LAN to the Internet. ■ Analog or ISDN Dial-up account. ■ Static IP Your ISP assigns or you have purchased a permanent IP address. ■ PPTP Your ISP uses Point-to-Point Tunneling Protocol (PPTP).
	HA Mode (Model 360/360R)	The following high availability modes are available for the WAN ports: ■ Normal Load balancing settings apply to the port when it is enabled and operational. ■ Off WAN port is not used at all. ■ Backup WAN port only passes traffic if the other WAN port is not functioning.
	Alive Indicator Server (Model 360/360R)	URL for a site to which the security gateway sends a PING or echo request to test for connectivity. If you do not specify a URL, the security gateway uses the address of the default gateway.

Table C-10 Main Setup tab field descriptions (Continued)

Section	Fields	Description
Optional Network Settings	Host Name	Name of the security gateway on the network. A default value based on the model number and the MAC address is provided in the Setup Wizard.
	Domain Name	Domain name by which external users can access the security gateway. For example, mysite.com.
	MAC Address	Physical (MAC) address of the security gateway. The default value is factory-set. You can change this value if your ISP is expecting a certain MAC address (MAC spoofing or cloning).

Static IP & DNS tab field descriptions

Use the Static IP & DNS tab to configure the security gateway to connect to the Internet with a static IP address and DNS servers, or to connect to your intranet.

Table C-11 Static IP and DNS tab field descriptions

Section	Field	Description
Model 320: WAN IP Model 360/360R: WAN 1 IP, WAN 2 IP	IP Address	Static IP address for your account. If you type an IP address, you must also type a netmask and a default gateway.
	Netmask	Netmask for your account. The netmask determines if packets are sent to the default gateway. If you type a netmask, you must also type an IP address and a default gateway.
	Default Gateway	IP address of the default gateway. The security gateway sends any packet it does not know how to route to the default gateway. If you type a default gateway, you must also type an IP address and a netmask.
Domain Name Servers	DNS 1, DNS 2, DNS 3	You must specify at least one, and up to three, DNS servers to use for resolving host and IP addresses.

PPPoE tab field descriptions

Use the PPPoE tab to configure the security gateway to connect to the Internet with an account that uses PPPoE for authentication.

Table C-12 PPPoE tab field descriptions

Section	Field	Description
Model 320: Sessions Model 360: WAN Port and Sessions	WAN Port (Model 360/360R)	Select the WAN port for which you are configuring PPPoE.
	Session	Lets you configure how the WAN port uses PPPoE. To configure a single-session PPPoE account, click Session 1, and then click Select. To configure a multi-session PPPoE account, select the session to configure, and then click Select.
Connection	Connect on Demand	Lets the security gateway create a connection to the PPPoE account only when an internal user makes a request, such as browsing to a Web page. This field, combined with Idle Time-out, is useful if your ISP charges are on a per-usage time basis.
	Idle Time-out	Number of minutes that the connection can remain idle (unused) before disconnecting. Type 0 to keep the connection always on and to prevent the security gateway from disconnecting. If the value is more than 0, check the Connect on Demand check box to reconnect automatically when needed. When combined with Connect on Demand, the connection to your ISP is only connected when a client is using it.
	Static IP Address	If you received a static IP address for your PPPoE account from your ISP, type it here.

Table C-12 PPPoE tab field descriptions (Continued)

Section	Field	Description
Choose Service	Query Services	When you click Query Services, the security gateway connects to your ISP and determines which services are available. You must disconnect from your PPPoE account before using this feature.
	Service	Select a service for the PPPoE account. To determine which services are available, click Query Services.
User Information	User Name	User name for the PPPoE account. This may be different from the account name. Some ISPs expect email address format for the user name, for example, johndoe@myisp.net.
	Password	Password for the PPPoE account.
	Verify Password	Retype the password for the PPPoE account.
Manual Control	Connect	Create a connection to the PPPoE account.
	Disconnect	Closes an open connection to the PPPoE account.

Dial-up Backup & Analog/ISDN tab field descriptions

The Dial-Up Backup & Analog/ISDN lets you configure the security gateway to connect to the Internet with a primary dial-up account, a primary dial-up ISDN account, or a back-up dial-up account.

Table C-13 Dial-up or ISDN tab field descriptions

Section	Field	Description
Backup Mode	Enable Backup Mode	If you use a dedicated account as your primary connection, you can specify a dial-up account as a backup, if the connection to the account fails.

Table C-13 Dial-up or ISDN tab field descriptions (Continued)

Section	Field	Description
ISP Account Information	User Name	User name for the dial-up account.
	Password	Password for the dial-up account.
	Verify Password	Retype the password for the dial-up account.
	IP Address	If you have a static IP address with your ISP, type it here. Otherwise, the ISP dynamically assigns you an IP address.
	Dial-up Telephone 1, Dial-up Telephone 2, Dial-up Telephone 3	Telephone number for the security gateway to dial to connect to the dial-up account. You must specify at least one, and up to three dial-up numbers. If Dial-up Telephone 1 fails to connect, the security gateway then dials Dial-up Telephone 2, and so on. If the security gateway must dial a 9 to get an outside line, type 9 and then a comma before the telephone number. For example: 9,18005551212. This text box allows numbers, commas, and spaces.

Table C-13 Dial-up or ISDN tab field descriptions (Continued)

Section	Field	Description
Modem Settings	Model	Model type of your modem. If your specific model type is not listed, click Other.
	Initialization String	Modem command that the security gateway sends to the modem to begin dialing the ISP. Specify this value only if you select Other as the modem model.
	Line Speed	Speed at which you want the modem to connect to the dial-up account. If the security gateway is having trouble connecting, lower the line speed.
	Line Type	Type of line for your account. ■ Dial Up Line This line type is typically used if a connection to the Internet is not connected all the time. ■ Leased line This line type provides a permanent connection to the Internet.
	Dial Type	Type of signal your modem uses to dial the dial-up telephone number. Options include: ■ pulse ■ tone ■ other
	Dial String	Modem command to begin dialing the dial-up telephone number.
	Idle Time-out	Number of minutes that the connection may remain idle (unused) before disconnecting.
	Redial String	Modem command that specifies to redial the dial-up telephone number if the initial connection fails.
Manual Control	Dial	Opens a connection to the dial-up account.
	Hang Up	Closes an open connection to the dial-up account.

Table C-13 Dial-up or ISDN tab field descriptions (Continued)

Section	Field	Description
Analog Status	Port Status	Describes the status of the serial port on the security gateway where the modem is connected. Possible port status includes: ■ Idle ■ Dialing ■ Internet Access ■ Hanging Up
	Physical Link	Indicates whether the modem is connected to the phone number. Possible physical link status include: ■ Off ■ On
	PPP Link	Possible PPP link status includes: ■ User Authenticated via PPP (User name/ password was correct) ■ Off ■ On
	PPP IP Address	IP address that is assigned to your account when you connect. If you have a static IP address, it is the same each time. If the ISP assigns IP addresses dynamically, the IP address may be different each time a connection is established. Possible PPP IP address values include: ■ 0.0.0.0 ■ IP from ISP where IP from ISP is the IP address dynamically allocated to you when you connect.
	Phone Line Speed	Speed at which the modem is connected to the ISP. Possible phone line speeds include: ■ Unknown ■ ##### where ##### is a number representing the phone speed. For example, 48800.

PPTP tab field descriptions

Configure the security gateway to connect to the Internet with an account that uses PPTP for authentication.

Table C-14 PPTP tab field descriptions

Section	Field	Description
WAN Port: Model 360/360R	WAN Port(Model 360/360R)	WAN port for which you are configuring PPTP.
Connection	Connect on Demand	When enabled, a connection is established only when a request is made, such as when a user browses to a Web page.
	Idle Time-out	Number of minutes that the connection can remain idle (unused) before disconnecting. Type 0 to keep the connection always on and to prevent the security gateway from disconnecting. For values greater than 0, check Connect on Demand to reconnect automatically when needed.
	Server IP Address	IP address of the PPTP server. The default value for the first octet is 10. The default value for the last octet is 138.
	Static IP Address	Only for static PPTP accounts. The static IP address for your account if you purchased one from, or are assigned one by, your ISP.
User Information	User Name	User name for your PPTP account.
	Password	Password for your PPTP account.
	Verify Password	Retype the password for your PPTP account.
Manual Control	Connect	Opens a connection to your PPTP account.
	Disconnect	Closes an open connection the PPTP account.

Dynamic DNS tab field descriptions

Dynamic DNS services let you use your own domain name (mysite.com, for example) or to use their domain name and your subdomain to connect to your services, such as a a VPN gateway, Web site or FTP. For example, if you set up a

virtual Web server and your ISP assigns you a different IP address each time you connect, your users can always access www.mysite.com.

Table C-15 Dynamic DNS tab field descriptions

Section	Field	Description
Service Type	Dynamic DNS Service	Service through which you get your dynamic DNS service. Options include: ■ TZO A dynamic DNS service. ■ Standard There are many standard dynamic DNS services. See the *Symantec Gateway Security 300 Series Release Notes* for the list of supported services. ■ Disable The security gateway does not use dynamic DNS.
	WAN Port (Model 360/360R)	WAN port to configure dynamic DNS.
	Force DNS Update	Sends updated IP information to the dynamic DNS service. Do this only if requested by Symantec Technical Support.
TZO Dynamic DNS Service	Key	Alphanumeric string of characters that acts as a password for the TZO account. TZO sends the key when the account is created. The maximum TZO key length is 16 characters.
	Email	Email address that acts as a user name with the TZO service.
	Domain	Domain name that you want to manage with the TZO service. For example, marketing.mysite.com.

Table C-15 Dynamic DNS tab field descriptions (Continued)

Section	Field	Description
Standard Service	User Name	User name for the account that you create with a dynamic DNS service.
	Password	Password for the account that you create with a dynamic DNS service.
	Verify Password	Retype the dynamic DNS account password.
	Server	IP address or DNS-resolvable name of the server that provides the dynamic DNS service. For example, members.dyndns.org.
	Host Name	Name to assign to the security gateway. For example, if you want marketing as the host name, and the domain name is mysite.com, you access the security gateway by marketing.mysite.com.
Standard Optional Settings	Wildcards	Enables external access to *.yoursite.yourdomain.com where: ■ * is a CNAME like www, mail, irc, or ftp. ■ yoursite is the host name. ■ yourdomain.com is your domain name.
	Backup MX	Enables a backup mail exchanger. If you check this check box, the mail exchanger you specify in the Mail Exchanger text box is used first; if it fails, the backup mail exchanger (supplied by the dynamic DNS service) takes its place.
	Mail Exchanger	Mail exchangers specify which server you want to handle email sent to a given domain name. For example, you have www.mysite.com and mail.mysite.com. You have your Web server configured to allow browsing to both www.mysite.com and mysite.com. You want email that comes to @mysite.com to be handled by the mail server and not the Web server. You set up a mail exchanger to redirect @mysite.com email to mail.mysite.com. Host names in mail exchangers cannot be CNAMEs. You cannot specify your mail exchanger using an IP address. Refer to your dynamic DNS service documentation for more information.

Routing tab field descriptions

Use the routing table to configure static or dynamic routing for your security gateway.

Table C-16 Routing tab field descriptions

Section	Field	Description
Dynamic Routing	Enable RIP v2	Enables dynamic routing. Use this only for intranet or department gateways.
Static Routes	Route Entry	Select an entry from the list to edit or delete.
	Destination IP	IP address/subnet for traffic requiring routing.
	Netmask	Mask (used with the destination IP address) to set range of IP addresses for traffic requiring routing.
	Gateway	IP address of the router to which to send traffic, that meets the IP address and mask combination of destination IP address and netmask.
	Interface	Appliance interface to which the defined traffic is routed. Options include: ■ Internal LAN ■ External WAN 1 ■ External WAN 2
	Metric	Integer representing the order in which you want the routing statement executed. For example, 1 is executed first.
Routing Table List	Destination	IP address/subnet for traffic requiring routing.
	Mask	Mask (used with the destination IP address) to set range of IP addresses for traffic requiring routing.
	Gateway	IP address of the router to which to send traffic, that meets the IP address and mask combination of destination IP address and netmask.
	Interface	Appliance interface to which the defined traffic is routed.
	Metric	Integer representing the order in which you want the routing statement executed. For example, 1 is executed first.

Advanced tab field descriptions

Use the Advanced tab to configure optional connection settings and the DNS gateway.

Table C-17 Advanced tab field descriptions

Section	Field	Description
Load Balancing	WAN 1 Load (Model 360/360R)	Percentage of traffic to pass through WAN 1. The remainder of traffic passes through WAN 2. For example, if you type 80%, WAN 1 passes 80% of the traffic and WAN 2 passes 20%. The default percentage is 50%.
	Bind SMTP with WAN Port (Model 360/360R)	Determines the WAN port (and subsequently, which ISP) through which email is sent. This is useful if you have two different ISPs configured, one for each WAN port. In this case, outgoing email is sent on the WAN port to which SMTP is bound. Outgoing mail sent by a client is sent on the WAN port that he is using, and therefore, sent through the ISP (connection type) that is configured for that port. Options include: ■ None (either) Sends email through either WAN port. ■ WAN1 Binds SMTP to WAN1. ■ WAN2 Binds SMTP to WAN2.

Table C-17 Advanced tab field descriptions (Continued)

Section	Field	Description
Optional Connection Settings	Idle Renew DHCP	Number of minutes after which, if there is no LAN-to-WAN or WAN-to-LAN traffic, the security gateway sends a request to renew the DHCP lease. To disable this feature, type 0.
	Force Renew (Model 320)	Sends a request to the ISP to renew the DHCP lease.
	Renew WAN1, Renew WAN2 (Model 360/360R)	Sends a request to the ISP to renew the DHCP lease for WAN1 or WAN2.
	WAN Port 1 WAN Port 2 (Model 360/360R)	Maximum size (in bytes) of packets that leave through the WAN port you are configuring. The default value is 1500 bytes. For PPPoE, the default value in bytes is 1472.
PPP Settings	Time-out	Number of seconds between echo requests.
	Retries	Number of times that the security gateway sends echo requests.
DNS Gateway	DNS Gateway	IP address of a non-ISP (private or internal) DNS gateway to use for name resolution.
	Enable DNS Gateway Backup	If you specify a DNS gateway and it becomes unavailable, this enables the appliance to use your ISP's DNS servers as a backup.

Firewall field descriptions

The Symantec Gateway Security 300 Series security gateway includes firewall technology that let you define the inbound and outbound rules governing the traffic that passes through the security gateway. When configuring the firewall you need to identify all nodes (computers) that are protected on your network.

This section contains the following topics:

- Computers tab field descriptions
- Computer Groups tab field descriptions
- Inbound Rules field descriptions
- Outbound Rules tab field descriptions

- Services tab field descriptions
- Special Application tab field descriptions
- Advanced tab field descriptions

Computers tab field descriptions

Before configuring outbound or inbound rules, you must identify the nodes on the Computers tab.

Table C-18 Computers tab field descriptions

Section	Field	Description
Host Identity	Host	Select a host name (network name) from the list to edit or delete.
	Host Name	Defines the name of the host (a computer on your internal network). Use a short descriptive name. You should use the host name or DNS name in the computer's network properties.
	Adapter (MAC) Address	Physical address of the host's network interface card (NIC), usually an Ethernet or wireless card.
	Computer Group	Displays all the computer groups to which you can bind hosts. Computer groups cluster computers to which you want to apply the same rules. Options include: ■ Everyone ■ Group 1 ■ Group 2 ■ Group 3 ■ Group 4

Table C-18 Computers tab field descriptions (Continued)

Section	Field	Description
Application Server	Reserve Host	Adds the MAC address (that you specified in the Adapter (MAC) Address text box) to the appliance's DHCP server so it is always assigned to the IP address that you specify in the IP Address text box. This is required for application servers. Checking this check box ensures that the DHCP server always offers the defined IP address to the computer you are defining, or you can set this IP address as a static address on the computer.
	IP Address	Defines the IP address of the application server.
Session Associations - Optional	Bind with WAN port (Model 360/ 360R)	Binds this computer to a particular WAN port so that its traffic only goes out through that WAN port. This is useful if you have two broadband accounts configured, one for each WAN port, and you want that computer's traffic to go through only one of the ISPs.
	Bind with PPPoE Session	Displays all the PPPoE sessions that you can bind to access groups and rules: ■ Session 1 ■ Session 2 ■ Session 3 ■ Session 4 ■ Session 5 Only select a session if your ISP service includes multiple PPPoE sessions.
Host List	Host Name	Name of the host (a computer on your internal network).
	Adapter (MAC) Address	Physical address of the host's network interface card (NIC), usually an Ethernet or wireless card.
	App Server	IP address of the application server.
	Computer Group	Computer group to which the host is assigned.
	PPPoE Session	PPPoE session to which the host is bound.

Computer Groups tab field descriptions

Computer groups help you group together computers (defined on the Computers tab) so that you can apply inbound and outbound rules.

Table C-19 Computer Groups tab field descriptions

Section	Field	Description
Security Policy	Computer Group	Select a computer group to edit or delete.
Antivirus Policy Enforcement	Enable Antivirus Policy Enforcement	If you enable AVpe for the selected computer group, the security gateway monitors client workstations to determine their compliance with current antivirus software and security policies. For each group, options include: ■ Warn Only (default) A client with non-compliant virus software or virus definitions is still allowed access. A log message warns the administrator that the client is non-compliant. ■ Block Connections A client with non-compliant virus software or virus definitions is denied access to the external network. The client is allowed access to the Symantec Antivirus CE Server or LiveUpdate server to bring their virus definitions into compliance.
Content Filtering	Enable Content Filtering	If you enable content filtering for the selected computer group, the security gateway allows or blocks access to URLs contained in the Content Filtering allow and deny lists. For each group, options include: ■ Use Deny List A list of blocked URLs, all others are allowed. ■ Use Allow List A list of URLs that permit access to the sites, all other sites are blocked.

Table C-19 Computer Groups tab field descriptions (Continued)

Section	Field	Description
Access Control (Outbound Rules)	No restrictions	A host assigned to this group may pass any traffic to the external network. You do not need to define rules for access groups in this category. The No Restrictions setting overrides any outbound rules. This is the default setting.
	Block ALL outbound access	When an access group is configured to block all Internet access behavior, all outbound traffic is blocked. A host assigned to this group may not pass any traffic through the security gateway. No rules need to be defined for access groups in this category. This is useful for nodes that only require access to the LAN and do not require access to the external network, for example network printers.
	Use rules defined in Outbound Rules Screen	When an access group is configured to use rules defined in the Outbound Rules tab, you must specify the type of traffic that the host, as a member of that logical group, may pass. Do this by creating an outbound rule. When this option is used, hosts are only allowed to pass traffic that matches the outbound rule list for that access group. The outbound default state of the security gateway is that all outbound traffic is blocked until the outbound rules are configured to allow certain kinds of outbound traffic.

Inbound Rules field descriptions

The Inbound Rules tab lets you define the traffic that can access your internal network.

Table C-20 Inbound Rules fields description

Section	Field	Description
Inbound Rules	Rule	Select an inbound rule to edit or delete.

Table C-20 Inbound Rules fields description (Continued)

Section	Field	Description
Rule Definition	Name	Type a new name when adding a rule.
	Enable Rule	Check to enable the inbound rule.
	Application Server	Shows the configured application servers available for inbound rules. These application servers are configured on the Computers tab.
	Service	Type of traffic applied to the rule. It includes both the list of predefined services and any custom services that you have created.
Inbound Rules List	Enabled?	Indicates whether the inbound rule is enabled for use.
	Name	Name of the inbound rule.
	Service	Service which this inbound rule governs, such as HTTP or FTP.

Outbound Rules tab field descriptions

The Outbound Rules tab defines traffic that can leave your network to access other networks or the Internet.

Table C-21 Outbound Rules tab field descriptions

Section	Field	Description
Computer Groups	Computer Group	Select a group to edit or add rules for the group.
Outbound Rules	Rule	Select an outbound rule to update or delete.
	Rule Name	Name of the outbound rule.
	Enable Rule	Check to enable the outbound rule.
	Service	Service which the outbound rule governs.
Outbound Rules List	Enabled?	Displays Y or N. Indicates whether the outbound rule is enabled for use.
	Name	Name of the outbound rule.
	Service	Service which the outbound rule governs.

Services tab field descriptions

Define the services to be used in the outbound and inbound firewall rules on the Services tab.

Table C-22 Services tab field descriptions

Section	Field	Description
Services	Application	Select an application available for services to edit or delete.
Application Settings	Name	Name of the service you are creating.
	Protocol	Select the protocol associated with the service. Options include: ■ TCP ■ UDP
	Listen on Port(s)	Defines the port range to listen for packets. ■ Start Type the first port in the range of listen on ports. ■ End Type the last port in the range of listen on ports. The quantity of ports in the range must match the Redirect to ports. For example, if you set the Listen on range to 20 to 27, the Redirect to range must also be 7 ports.
	Redirect to Port(s)	Defines the port range to where the packets are redirected. ■ Start Type the first port in the range of redirect to ports. ■ End Type the last port in the range of redirect to end ports. The quantity of ports in the range must match the Listen on ports. For example, if you set the Redirect to range to 20 to 27, the Listen on range must also be 7 ports.

Table C-22 Services tab field descriptions (Continued)

Section	Field	Description
Service List	Name	Name of the service.
	Protocol	Protocol associated with the service.
	Listen on Start Port	First port in the range to listen on.
	Listen on End Port	Last port in the range to listen on.
	Redirect to Start Port	First port in the range to which to redirect.
	Redirect to End Port	Last port in the range to which to redirect.

Special Application tab field descriptions

Certain applications with two-way communication (games, video or teleconferencing) require dynamic ports on the security gateway. Use the Special Applications tab to define those applications.

Table C-23 Special Applications tab field descriptions

Section	Field	Description
Special Applications	Application	Select a special application to update or delete.

Table C-23 Special Applications tab field descriptions (Continued)

Section	Field	Description
Special Application Settings	Name	Name of the special application.
	Enable	Enables the special application for all computer groups.
	Outgoing Protocol	Protocol for the outgoing packets. Options include: ■ TCP ■ UDP
	Outgoing Port(s)	Range of ports on which the packets are sent. ■ Start First port in the range of outgoing ports. ■ End Last port in the range of outgoing ports.
	Incoming Protocol	Protocol for the incoming packets. Options include: ■ TCP ■ UDP
	Incoming Port(s)	Range of ports on which the packets are received. ■ Start First port in the range of incoming ports. ■ End Last port in the range of incoming ports.

Table C-23 Special Applications tab field descriptions (Continued)

Section	Field	Description
Special Application List	Name	Name of the special application.
	Enabled	Indicates whether the special application is enabled for all computer groups.
	Outgoing Protocol	Protocol for the outgoing packets.
	Outgoing Start Port	First port in the range of outgoing ports.
	Outgoing End Port	Last port in the range of outgoing ports.
	Incoming Protocol	Protocol for the incoming packets.
	Incoming Start Port	First port in the range of incoming ports.
	Incoming End Port	Last port in the range of incoming ports.

Advanced tab field descriptions

You configure advanced firewall settings, such as IPsec pass-thru, on the Advanced tab.

Table C-24 Advanced tab field descriptions

Section	Field	Description
Optional Security Settings	Enable IDENT Port	Disabling the IDENT port makes port 113 closed, not stealth (not open). You should enable this setting only if there are problems accessing a server. The IDENT port normally contains the host name or company name information. By default, the security gateway sets all ports to stealth mode. This makes a computer to appear invisible outside of the network. Some servers, such as some email or MIRC servers, view the IDENT port of the system accessing them.
	Disable NAT Mode	Disabling NAT mode disables the firewall security functions. Only use this setting for intranet security gateway deployments where, for example, the security gateway is used as a bridge on a protected network. When the security gateway is configured for NAT mode, it behaves as an 802.1D bridge device.
	Block ICMP Requests	Blocks ICMP requests, such as PING and traceroute, to the WAN ports.

Table C-24 Advanced tab field descriptions (Continued)

Section	Field	Description
IPSec Passthru Settings	IPSec Type	These values are used in ESP IPsec VPNs from some vendors for their software clients for IPsec pass-thru compatability. These settings do not apply to the VPN gateway on the security gateway. Keep this setting at 2 SPI unless instructed by Symantec Technical Support to change it. The None setting lets VPN clients be used in exposed host mode if it is having problems connecting from behind the security gateway. Options include: ■ 1 SPI ADI (Assured Digital) ■ 2 SPI Normal (Cisco Client, Symantec Client VPN, Nortel Extranet, Checkpoint SecureRemote) ■ 2 SPI-C (Cisco VPN Concentrator 30x0 series (formerly Altiga) ■ Others Redcreek Ravlin Client ■ None Use only for debugging clients.
Exposed Host	Enable Exposed Host	Check to enable an exposed host. Activate this feature only when required. This lets one computer on a LAN have unrestricted two-way communication with Internet servers or users. This feature is useful for hosting games or special server or application.
	LAN IP Address	IP address of the exposed host. If a host is defined as an exposed host, all traffic not specifically permitted by an inbound rule is automatically redirected to the exposed host.

VPN field descriptions

Virtual Private Networks (VPNs) let you securely extend the boundaries of your internal network to use insecure communication channels (such as the Internet)

to safely transport sensitive data. VPNs are used to allow a single user or a remote network access to the protected resources of another network.

The Symantec Gateway Security 300 Series security gateways support two types of VPN tunnels: Gateway-to-Gateway and Client-to-Gateway.

This section contains the following topics:

- Dynamic Tunnels tab field descriptions
- Static Tunnels tab field descriptions
- Client Tunnels tab field descriptions
- Client Users tab field descriptions
- VPN Policies tab field descriptions
- Status tab field descriptions
- Advanced tab field descriptions

Dynamic Tunnels tab field descriptions

This table describes the fields on the Dynamic Tunnels tab you use to configure dynamic Gateway-to-Gateway VPN tunnels.

Table C-25 Dynamic Tunnels field descriptions

Section	Field	Description
IPsec Security Association	VPN Tunnel	Select a tunnel to update or delete.
	Name	Name of the tunnel. The tunnel name can be up to 25 alphanumeric characters, dashes, and underscores. This name used only for reference within the SGMI. You can create up to 50 tunnels.
	Enable VPN Tunnel	Enables VPN users to use the tunnel you are defining. To temporarily disable the tunnel, uncheck this box and click Update. To permanently disable the tunnel, click Delete.
	Phase 1 Type	Mode of phase 1 negotiation. Options include: ■ Main Mode Negotiates with a source IP address. ■ Aggressive Mode Negotiates with an identifier such as a name. Client VPN software typically negotiates in aggressive mode. The default value is Main Mode.
	VPN Policy	Policy that dictates authentication, encryption, and timeout settings. The list contains Symantec pre-defined policies and any policies you created on the VPN Policies tab.

Table C-25 Dynamic Tunnels field descriptions

Section	Field	Description
Local Security Gateway	PPPoE Session	The default PPPoE session is Session 1. This requires an ISP PPPoE account. If you have a single-session PPPoE account, leave the PPPoE session at Session 1.
	Local Endpoint (Model 360/360R)	Port on the security gateway where you want the tunnel to end. Options include: ■ WAN1 ■ WAN2
	ID Type	ID type used for ISAKMP negotiation. Options include: ■ IP Address ■ Distinguished Name The default value is IP Address.
	Phase 1 ID	Value that corresponds to the ID Type. This value is used to identify the security gateway during phase 1 negotiations. If you selected IP address, type an IP address. If you selected Distinguished Name, type a fully qualified domain name. If you select IP address and leave this field blank, the default value is the IP address of the security gateway's internal interface. The maximum value is 31 alphanumeric characters.
	NetBIOS Broadcast	Allows browsing of the VPN network in the Network Neighborhood and file sharing on a Microsoft Windows computer. A WINS host is needed to accept the traffic. NetBIOS broadcast is disabled by default.

Table C-25 Dynamic Tunnels field descriptions

Section	Field	Description
	Global Tunnel	Normally, only requests destined to the network protected by the remote VPN Gateway are forwarded through the VPN. Other traffic, like Web browsing are forwarded straight out into the Internet. Enabling Global Tunnel forces all external traffic to the above VPN Gateway. This allows the Main office's firewall to filter traffic before sending the request on into the Internet. This provides your remote site with firewall protection from the Main site. Destination Networks should be blank with Global Tunnel enabled. Enabling Global Tunnel will also Disable all other SAs since all traffic must be routed through the global tunnel gateway. The global tunnel is disabled by default.

Table C-25 Dynamic Tunnels field descriptions

Section	Field	Description
Remote Security Gateway	Gateway Address	IP address or fully qualified domain name of the remote gateway (the gateway to which the tunnel will connect). The maximum number of alphanumeric characters for this text box is 128.
	ID Type	ID type used for ISAKMP negotiation. Options include: ■ IP Address ■ Distinguished Name The default value is IP Address.
	Phase 1 ID	Value that corresponds to the ID Type. If you selected IP address, type an IP address. If you selected Distinguished Name, type a fully qualified domain name. The maximum number of alphanumeric characters in this text box is 31.
	Pre-Shared Key	Key for authenticating ISAKMP (IKE). It authenticates the remote end of the tunnel. The pre-shared key is between 20 and 64 alphanumeric characters. The pre-shared key on the remote end of this tunnel must match this value.
	Remote Subnet IP	IP address of the remote subnet.
	Mask	Mask of the remote subnet.

Static Tunnels tab field descriptions

This table describes the fields on the Static Tunnels tab that you use to

configure static gateway-to-gateway VPN tunnels for the security gateway.

Table C-26 Static Tunnel tab field descriptions

Section	Field	Description
IPSec Security Association	VPN Tunnel	Select a tunnel to update or delete.
	Tunnel Name	Name of the static tunnel. This name is only used for reference within the SGMI. You can create up to 50 static tunnels. The maximum tunnel name is 50 characters.
	Enable VPN Tunnel	Enables VPN users to use the tunnel you are defining. To temporarily disable the tunnel, uncheck this box, and then click Update. To permanently disable the tunnel, click Delete.
	PPPoE Session	This requires an ISP PPPoE account. The default PPPoE session is Session 1. If you have a single-session PPPoE account, leave the PPPoE session at Session 1.
	Local Endpoint (Model 360)	Port on the security gateway on which you are working where you want the tunnel to end.
	Incoming SPI	Incoming security parameter index on the IPsec packet. The default value is a decimal number. Prepend the value with 0x for hex numbers. The Security Parameter Index (SPI) is a number between 257 and 8192 that identifies the tunnel. This value must match the Outgoing SPI on the remote end of the tunnel.
	Outgoing SPI	Outgoing security parameter index on the IPsec packet. The default value is a decimal number. Prepend the value with 0x for hex numbers. The Security Parameter Index (SPI) is a number between 257 and 8192 that identifies the tunnel. This is the SPI with which packets are sent. This value must match the incoming SPI on the remote end of the tunnel.
	VPN Policy	Policy that dictates authentication, encryption, and timeout settings. The list contains Symantec pre-defined policies and any policies you created on the VPN Policies tab.

Table C-26 Static Tunnel tab field descriptions (Continued)

Section	Field	Description
Remote Security Gateway	Gateway Address	IP address or fully qualified domain name of the security gateway to which you are creating a tunnel. The maximum length for this field is 128 alphanumeric characters.
	NetBIOS Broadcast	Allows browsing of the VPN network in the Network Neighborhood and file sharing on a Microsoft Windows computer. A WINS host is needed to accept the traffic. NetBIOS is disabled by default.
	Global Tunnel	Normally, only requests destined to the network protected by the remote VPN gateway are forwarded through the VPN. Other traffic, like Web browsing are forwarded straight out into the Internet. Enabling Global Tunnel forces all external traffic to the above VPN gateway. This allows the Main office's firewall to filter traffic before sending the request on into the Internet. This provides your remote site with firewall protection from the Main site. Destination networks should be blank with Global Tunnel enabled. Enabling Global Tunnel also disables all other SAs since all traffic must be routed through the global tunnel gateway. The global tunnel is disabled by default.
	Remote Subnet IP	IP address of the remote subnet.
	Mask	Mask of the remote subnet.

Client Tunnels tab field descriptions

Use the Client Tunnels tab to define client-to-gateway tunnels. Ensure that you have defined your users on the Client Users tab before defining the tunnel.

Table C-27 Client tunnel tab definition field descriptions

Section	Field	Description
Group Tunnel Definition	VPN Group	Select a VPN Group to update or delete. You can modify the membership of these three groups. You cannot add VPN groups.
	Enable client VPNs on WAN side	Lets defined VPN users connect to the WAN interface.
	Enable client VPNs on WLAN/ LAN side	Lets defined VPN users connect to LAN and wireless LAN interface.
VPN Network Parameters	Primary DNS	IP address of the primary DNS server that the VPN user uses for name resolution.
	Secondary DNS	IP address of the secondary DNS server that the VPN user uses for name resolution.
	Primary WINS	IP address of the primary WINS server. Windows Internet Naming Service (WINS) is a system that determines the IP address associated with a particular network computer.
	Secondary WINS	IP address of the secondary WINS server.
	Primary Domain Controller (PDC)	IP address of the Primary Domain Controller.

Table C-27 Client tunnel tab definition field descriptions (Continued)

Section	Field	Description
Extended User Authentication	Enable Extended User Authentication	Requires that all users in the selected VPN group use RADIUS for extended authentication after phase 1, but before phase 2.
	RADIUS Group Binding	If a RADIUS group binding is specified, the remote user must be a member of that group on the RADIUS Server. The filter ID returned from RADIUS must match this value to authenticate the user. When specifying RADIUS group bindings, no two client tunnels may have the same setting for the group binding. The maximum length of the value is 25 characters.
WAN Client Policy	Enable Content Filtering	Traffic for all clients in the selected VPN group is subject to the content filtering rules set forth in the allow and deny lists.
	Use Deny List	Content filtering uses the deny list, a list of URLs that clients are not permitted to view, allowing all other traffic.
	Use Allow List	Content filtering uses the allow list, a list of URLs that clients are permitted to view, blocking all other traffic.
	Enable Antivirus Policy Enforcement	Requires that all users in the selected VPN group have antivirus software with the most current virus definitions.
	Warn Only	If the user does not have antivirus software with the most current virus definitions, a text message is logged.
	Block Connections	If the user does not have antivirus software with the most current virus definitions, the traffic is not permitted.

Client Users tab field descriptions

Use the Client Users tab to define remote users that will access your network with a VPN tunnel.

Table C-28 Client Users tab field descriptions

Section	Field	Description
VPN User Identity	User	Select a user to update or delete.
	Enable	Lets a user use a VPN tunnel. To temporarily suspend a user, uncheck Enable, and then click Update. To permanently remove a user, click Delete.
	User Name	User name for the client user. The maximum number of alphanumeric characters for this value is 31. It must match the remote Client ID in Symantec Client VPN software. You can add up to 50 client users.
	Pre-Shared Key	ISAKMP (IKE) authenticating key. The key is unique to this user. You must enter a pre-shared key. The maximum number of alphanumeric characters for this value is 64. The pre-shared key must match the pre-shared key offered by remote VPN client.
	VPN Group	Defines the VPN Group (tunnel definition) that for this user.

VPN Policies tab field descriptions

You select one VPN policy for each tunnel. Use the VPN Policies tab to define each policy, or to edit a default policy.

Table C-29 VPN policies field descriptions

Section	Field	Description
IPsec Security Association (Phase 2) Parameters	VPN Policy	Select a policy to update or delete. **Note:** You cannot delete Symantec pre-defined policies. Options include: ■ ike_default_crypto ■ ike_default_crypto_strong ■ Static_default_crypto ■ Static_default_crypto_strong ■ Any VPN policies you created
	Name	Name to assign to the policy. This name is used for SGMI reference only. The maximum value is 28 alphanumeric characters.
	Data Integrity (Authentication)	Options include: ■ ESP MD5 (default) ■ ESP SHA1 ■ AH MD5 ■ AH SHA1 This selection must match the remote security gateway.
	Data Confidentiality (Encryption)	Options include: ■ DES ■ 3DES ■ AES_VERY_STRONG ■ AES_STRONG ■ AES ■ NULL (none) If you have selected an AH Data Integrity Authentication, you do not need to select an encryption type.

Table C-29 VPN policies field descriptions (Continued)

Section	Field	Description
	SA Lifetime	Time, in minutes, before phase 2 renegotiation of new encryption and authentication keys for the tunnel. The default value is 480 minutes. The maximum value is 2,147,483,647 minutes.
	Data Volume Limit	Maximum number of kilobytes allowed through a tunnel before a rekey is required. The default value is 2100000 KB (2050 MB). The maximum value is 4200000 KB (4101 MB).
	Inactivity Time-out	Number of minutes a tunnel can be inactive before it is re-keyed. Type 0 for no timeout.
	Perfect Forward Secrecy	PFS provides additional protection from attackers trying to guess the current ISKAMP key. Not all clients and security gateways are compatible with Perfect Forward Secrecy. Options include: ■ DH Group 1 ■ DH Group 2 ■ DH Group 5

Status tab field descriptions

The Status tab shows the status of your VPN tunnels and client users.

Table C-30 Status tab field descriptions

Section	Field	Description
Dynamic VPN Tunnels	Status	Status of the selected tunnel.
	Name	Name of the selected tunnel.
	Negotiation Type	Configured negotiation type. This field applies to dynamic VPN tunnels only.
	Security Gateway	Name of the selected security gateway.
	Remote Subnet	Address of the remote subnet.
	Encryption Method	Configured encryption method.
Static VPN Tunnels	Status	Displays connected or disconnected.
	Name	Name of the selected static tunnel.
	Security Gateway	IP address of the remote gateway to which the tunnel is connected.
	Remote Subnet	Subnet of the remote gateway to which the tunnel is connected.
	Encryption Method	Authentication method for this tunnel.

Advanced tab field descriptions

Use the Advanced tab to configure advanced VPN settings for phase 1 negotiation, which applies to all clients.

Table C-31 Advanced tab field descriptions

Section	Field	Description
Global VPN Client Settings	Local Gateway Phase 1 ID Type	Phase 1 ID (ISAKMP) used by local gateway for VPN clients. Options include: ■ IP Address If you select IP Address, leave the Local Gateway Phase 1 ID text box blank. ■ Distinguished Name If you select Distinguished Name, in Local Gateway Phase 1 ID text box, type a local gateway Phase 1 ID to be used by all clients.
	Local Gateway Phase 1 ID	Value that corresponds to the ID Type. If you selected IP address, leave this text box blank. If you selected Distinguished Name, type a fully qualified domain name. Any client connected to the security gateway must use this Phase 1 ID when defining his or her remote gateway endpoint on the client. The maximum value is 31 alphanumeric characters.
	VPN Policy	VPN policy for VPN client tunnels for phase 2 tunnel negotiation. The list shows pre-defined Symantec policies and any policies you created on the VPN Policies tab.
Dynamic VPN Client Settings	Enable Dynamic VPN Client Tunnels	Lets undefined VPN clients connect to the security gateway for extended authentication.
	Pre-shared Key	Key for authenticating ISAKMP (IKE). It authenticates the remote end of the tunnel. The pre-shared key is between 20 and 64 alphanumeric characters. The pre-shared key on the remote end of this tunnel must match this value.

Table C-31 Advanced tab field descriptions (Continued)

Section	Field	Description
Global IKE Settings (Phase 1 Rekey)	SA Lifetime	Time, in minutes, before phase 1 renegotiation of new encryption and authentication keys for the tunnel. The default value is 1080 minutes. The maximum value is 2,147,483,647 minutes.
RADIUS Settings	Primary RADIUS Server	IP address or fully qualified domain name of the server used to process extended authentication exchanges with VPN clients. The maximum values is 128 alphanumeric characters.
	Secondary RADIUS Server	IP address or fully qualified domain name of the alternate server used to process extended authentication exchanges with VPN clients. The maximum values is 128 alphanumeric characters.
	Authentication Port (UDP)	Port on the RADIUS server used for authentication. The default value is 1812. The maximum value is 65535.
	Shared Secret or Key	Authentication key used by the RADIUS server. The maximum value is 50 alphanumeric characters.

IDS/IPS field descriptions

The Symantec Gateway Security 300 series security gateway provides intrusion detection and prevention (IDS/IPS). The IDS/IPS functions are enabled by default, and provide atomic packet protection with spoof protection and IP. You may disable IDS/IPS functionality at any time.

The following types of protection are offered with the IDS/IPS feature:

- IP spoofing protection
- IP options verification
- TCP flag validation
- Trojan horse protection

- Port scan detection

This section contains the following topics:

- IDS Protection tab field descriptions
- Advanced tab field descriptions

IDS Protection tab field descriptions

Configure basic IDS protection on the IDS Protection tab.

Table C-32 IDS Protection tab field descriptions

Section	Field	Description
IDS Signatures	Name	Select a signature to update. * Asterisk indicates Trojan port detection. Warning and Block is disabled if traffic is explicitly allowed in Inbound Rules.
Protection Settings	Block and Warn	If an attack is detected, blocks the traffic and logs a message.
	Block/Don't Warn	If an attack is detected, blocks the traffic without a logging a message.
	WAN	Enables WAN protection.
	WLAN/LAN	Enables wireless LAN and LAN protection.
Protection List	Attack Name	Name of the IDS signatures.
	Block and Warn	Displays Y for yes or N for no. Indicates if the Block and Warn protection setting is enabled for this signature.
	Block/Don't Warn	Displays Y for yes or N for no. Indicates if the Block/Don't Warn protection setting is enabled for this signature.
	WAN	Displays Y for yes or N for no. Indicates if the WAN is protected.
	WLAN/LAN	Displays Y for yes or N for no. Indicates if the wireless LAN and LAN is protected.

Advanced tab field descriptions

Configure spoof protection on the Advanced tab.

Table C-33 Advanced tab field descriptions

Section	Field	Description
IP Spoof Protection	WAN	Enables spoof protection on the LAN.
	WLAN/LAN	Enables spoof protection on the wireless LAN and LAN.
TCP Flag Validation	TCP Flag Validation	Blocks and logs any traffic with illegal flag combinations for traffic that is not being denied by the security policy. Any traffic denied by the security policy that has one or more bad TCP flag combinations is classified as one of several NMAP port scanning techniques (NMAP Null Scan, NMAP Christmas Scan, and so on).

AVpe field descriptions

The AVpe feature lets you monitor client AVpe configurations and, if necessary, enforce security policies to restrict network access to only those clients who are protected by antivirus software with the most current virus definitions.

Table C-34 AVpe tab field descriptions

Section	Field	Description
Server Location	Primary AV Master	Defines the primary antivirus server in your network. This is the server to which you want the security gateway to connect to verify client virus definitions.
	Secondary AV Master	Defines a secondary antivirus server. The security gateway connects to this server to verify client virus definitions if it cannot access the primary antivirus server.
	Query AV Master Every	Type an interval (in minutes) for the security gateway to query the antivirus server. For example, if you type 10 minutes, the security gateway queries the antivirus server every 10 minutes to obtain the latest virus definition list. The default setting is 10 minutes. You must enter a value greater than 0.
	Query Master	This button lets you override the time interval set in the Query AV Server Every field. When clicked, the security gateway queries the antivirus server for the latest virus definitions. Before you click this button, enter the primary and secondary AV master IP addresses, and then click Save. When first enabling AVpe, use this button to force the security gateway to connect to the primary or secondary antivirus server to obtain current virus definitions.

Table C-34 AVpe tab field descriptions (Continued)

Section	Field	Description
Policy Validation	Verify AV Client is Active	When enabled, this field lets you verify that Symantec antivirus software is installed and active on a client's workstation. Options include: ■ Latest Product Engine (default) Verifies that Symantec antivirus software is active and that it contains the latest product scan engine. ■ Any Version Verifies that Symantec antivirus software is active with any qualified version of the product scan engine. **Note:** Make sure UDP/Port 2967 is allowed by personal firewalls.
	Verify Latest Virus Definitions	Lets you verify whether the latest virus definitions are installed on a client's workstation before allowing network access. This field is enabled by default.
	Query Clients Every	Type an interval (in minutes) for the security gateway to query client workstations to verify virus definitions. For example, if you type 10 minutes, the security gateway queries the client workstations every 10 minutes to verify that their workstations have the latest virus definitions applied. The default setting is 480 minutes (8 hours).

Table C-34 AVpe tab field descriptions (Continued)

Section	Field	Description
AV Master Status	AV Master	Identifies the antivirus server (either primary or secondary) for which summary information is displayed.
	Status	Indicates the operational status of the antivirus server. Up is displayed when the server is online and functional; Down is displayed when the server is offline.
	Last Update	Displays the date (numerically) when the security gateway last queried the server for virus definition files; for example: 5/14/2003.
	Host	Displays the IP address (or qualified domain name) of the primary or secondary antivirus server.
	Product	Displays the current product version of the Symantec AntiVirus Corporate Edition that the antivirus server is running; for example: 7.61.928.
	Engine	Displays the current version of the Symantec AntiVirus Corporate Edition scan engine that is running on the antivirus server; for example: NAV 4.1.0.15.
	Pattern	Displays the latest version of the virus definition file on the antivirus server; for example: 155c08 r6 (5/14/2003).

Table C-34 AVpe tab field descriptions (Continued)

Section	Field	Description
AV Client Status	AV Client	IP address of DHCP clients.
	Policy	Displays On or Off. Indicates whether the client has antivirus policies enforced.
	Status	Indicates whether the client is compliant.
	Group	Computer group to which the client is assigned.
	Last Update	Date and time of the last time the client's antivirus compliance was checked.
	Product	Name of the Symantec antivirus product that the client is using.
	Engine	Version of the scan engine in the Symantec antivirus product the client is using.
	Pattern	Version of the client's most recent virus definitions.

Content filtering field descriptions

The security gateway supports basic content filtering for outbound traffic. You use content filtering to restrict the content to which clients have access. For example, to restrict your users from seeing gambling sites, you configure content filtering to deny access to gambling URLs that you specify.

Table C-35 Content filtering configuration fields

Section	Field	Description
Select List	List Type	The possible list types include: ■ Deny ■ Allow A deny list specifies content that you do not want your clients to view. An allow list specifies the content that you permit your clients to view. Select a list, and then click View/Edit.

Table C-35 Content filtering configuration fields

Section	Field	Description
Modify List	Input URL	Type a URL to add to the deny or allow list. For example, www.symantec.com or myadultsite.com/mypics/me.html The maximum length of a URL is 128 characters. Each filtering list can hold up to 100 entries. You add URLs one at a time. You must use a fully qualified domain name. Content filtering cannot be performed using an IP address.
	Delete URL	On the drop-down list, select a URL that you want to delete, and then click Delete Entry.
Current List	URL	Depending on the list that you selected, shows all the URLs entered for that list.

Index

Numerics

3DES 93

A

administration password 16
administrative access 15
Advanced connection settings 43
advanced options 76
advanced protection settings 117
advanced WAN/ISP settings 50
AES-128 93
AES-192 93
AES-256 93
alive indicator 28, 40, 53
all.bin 129
allow list 111
analog 29
Analog connections 29
antivirus clients 109
antivirus server status 109
app.bin firmware 125
appliance, front panel LEDs 136
Asymmetrical Digital Subscriber Line (ASDL) 31
atomic IDS/IPS signatures 115
attack prevention 115
    Back Orifice 116
    Girlfriend 116
    Trojan horse 116
attacks 115
automatic updates 126
AVpe 104
    configuring 105
    log messages 110

B

Back Orifice 116
backing up and restoring
    configurations 133
backup dial-up account 39, 42
BattleNet 74
Bonk 116
broadband accounts 29
broadband connection 29

C

cable modem connectivity 29, 30
change
    appliance LAN IP address 58
    DHCP IP address range 60
Client-to-Gateway tunnels 96
Client-to-Gateway tunnels, global policy
  settings 101
clusters
    creating tunnels to Symantec Gateway 5400
      Series clusters 91
compression, tunnel 82
computer group membership 65
computer groups defining 67
computers and computer groups 64
configuration, backing up and restoring 133
configure password 16
configuring
    advanced connection settings 43
    advanced options 76
    advanced PPP settings 44
    advanced protection settings 117
    advanced WAN/ISP settings 50
    appliance as DHCP server 58
    AVpe 105
    Client-to-Gateway tunnels 96
    computers 65
    connection to the outside network 23
    connectivity 30
    dial-up accounts 40
    dynamic Gateway-to-Gateway tunnels 91
    exposed host 78
    failover 52
    Gateway-to-Gateway tunnels 88
    idle renew 43
    internal connections 57
    log preferences 120

Maximum Transmission Unit (MTU) 45
new computers 65
port assignments 60
PPTP 36
remote management 17
routing 48
special applications 74
static IP 35
static route entries 49
WAN port 28
configuring LAN IP settings 57
connecting manually, PPPoE 34
connection to the outside network 23
connection types, understanding 28
connection, network examples 24
connectivity,configuring 30
content filtering 111
allow list 111
deny lists 111
LAN 113
managing lists 112
WAN 100, 113
creating
custom phase 2 VPN policies 84
security policies 82

D

default settings, restore port assignment 61
defining
computer group membership 65
inbound access 68
outbound access 69
deny list 111
DES 93
DHCP 29
disabling 59
enabling 59
Force Renew 176
IP address range 60
usage 60
DHCP server 58
DHCP settings
advanced settings 43
dial-up accounts 39
backup 42
back-up account 39
configuring 40
connecting manually 42
monitoring status 43
verifying connectivity 42
dial-up connection 29
disabling
dynamic DNS 48
NAT mode 77
disconnect
idle PPPoE connections 31
DNS gateway 53
documentation
online help 13
DSL 29
DSL connectivity 29, 30
dual-WAN port 27
dynamic DNS
disabling 48
forcing updates 47
TZO 45
dynamic gateway-to-gateway tunnels 91
dynamic routing 48

E

Email Log Now 120
emailing log messages 120
enabling
IDENT port 76
IPsec pass-thru 77
enabling DHCP 59
exposed host 78

F

failover 52
Fawx 116
firewall,Host List 66
firmware 16, 126, 129
app.bin 125
updates 124
upgrading manually 129
flash the firmware 131
flashing 16
Force Renew 176
forcing dynamic DNS updates 47
front panel LEDs 136

G

games 74
Gateway-to-Gateway 88
dynamic tunnels 91

tunnel persistence and high-availability 90
gateway-to-gateway
supported VPN tunnels 90
Girlfriend 116
Global IKE Policy 83
global policy settings, Client-to-Gateway
tunnels 101

H

HA. *See* high availability
help 13
high availability 50
Host List 66
HTML buffer overflow 116

I

ICMP requests 40, 79
IDENT port 76
idle renew 43
IDS/IPS 115
IKE tunnels, Gateway-to-Gateway 91
inbound rules 68
internal connections 57
IP spoofing protection 117
IPsec pass-thru 77
ISDN connection 29
ISDN connections 29

J

Jolt 116

L

LAN IP address 58
LAN IP settings 57
Land 116
language selection 27
LB. *See* load balancing
LEDs 136
Licensing 145
LiveUpdate 131
server 127
updates 126
load balancing 51
log messages 124
log messages,email forwarding 120
log preferences 120

M

Main menu 14
managing
administrative access 15
content filtering lists 112
ICMP requests 79
using the serial console 19
manual dial-up accounts 42
manually
connect to PPTP account 38
upgrading firmware 129
manually reset password 17
Maximum Transmission Unit (MTU) 45
modem connectivity 40
monitoring
antivirus server status 109
DHCP usage 60
dial-up accounts 43
monitoring VPN tunnel status 102

N

NAT mode 77
Nestea 116
network access,planning 63
network connections 28
network settings
optional 54
network traffic control 63
network traffic control,advanced 103
Newtear 116
Norton Internet Security 130

O

online help 13
optional network settings 54
outbound rules 69
outside network
configuring connection 23
Overdrop 116

P

password
administration 16
configure 16
manually reset 17
PING 40
Ping of Death 116

planning network access 63
Point to Point Protocol over Ethernet. *See* PPPoE
Point-to-Point Protocol over Ethernet (PPPoE) 31
Point-to-Point-Tunneling Protocol (PPTP) 36
policy,Global IKE 83
Port assignments 60
Portal of Doom 116
PPP settings,advanced 44
PPPoE
    connecting manually 34
    connectivity 29
    Query Services 167
    verifying connectivity 33
PPTP
    configuring for connectivity 36
    connecting manually 38
    manual connection 38
    TCP/IP based network 36
    verifying connectivity 37
PPTP connection 30
preventing attacks 115
protection
    IP spoofing 117
    TCP flag validation 118
protection preferences
    configuring
        protection preferences settings 116
    settings 116

Q

Query Services 167
question mark 13

R

rear panel
    320 appliance 39
    360 and 360R 39
redirecting services 73
remote gateway administrator, sharing information 96
remote management 17
resetting the appliance 135
restore port assignment default settings 61
routing 48
routing,dynamic 48

S

scroll lock 19
secure VPN connections 81
Security Gateway Management Interface 15
Security Gateway Management Interface (SGMI) 13
security policies 82
serial console 19
    HyperTerminal 19
    scroll lock 19
Setup Wizard 27
    language selection 27
SGMI 15
signatures,atomic 115
SMTP binding 52
SMTP time-outs 76
special applications 74
special phone line
    ISDN 29
static gateway-to-gateway tunnels 93
Static IP 30
static IP
    configuring 35
static route entries 49
subnet 90
SubSeven 116
Symantec Gateway Security 5400 Series 90, 91
Syndrop 116

T

T1 connectivity 30
T3 29
TCP flag validation 118
TCP/IP-based network,PPTP 36
TCP/UDP flood protection 116
Teardrop 116
technical support 144
testing connectivity 52
TFTP 130
time-outs, SMTP 76
traffic flow
    inbound access 68
    outbound access 69
Trojan horse protection 116
Troubleshooting 141
tunnel compression 82
tunnel configurations
    VPN
        gateway-to-gateway 89

tunnel negotiations
Phase 1 83
Phase 2 83
tunnels
Client-to-Gateway 96
dynamic Gateway-to-Gateway 91
TZO 45

U

understanding connection types 28
updating firmware 124
upgrading firmware
Norton Internet Security 130

V

verifying PPPoE connectivity 33
video conferencing 74
VPN
authentication key lengths 93
configuring Client-to-Gateway tunnels 96
creating custom phase 2 policies 84
creating tunnels to Symantec Gateway Security 5400 Series clusters 91
encryption key lengths 93
global policy settings 101
monitoring tunnel status 102
phase 2, configurable 83
policies 82
secure connections 81
subnet 90
supported gateway-to-gateway tunnels 90
tunnel compression 82
tunnel configurations 89
Client-to-Gateway 96
gateway-to-gateway 89
tunnel high-availability 90
tunnel negotiations
Phase 1 83
Phase 2 83
tunnel persistence 90
tunnel status 102
VPN tunnel
remote management 17

W

WAN port
configuring MTU 45
connection 23
WAN port configuration 28
WAN/ISP
advanced settings 50
configuring idle renew 43
multiple IP addresses 31
Winnuke 116